

GRAVUN DATA PROCESSING ADDENDUM

Effective Date: _____

This Data Processing Addendum (“**DPA**”) forms part of the agreement governing access to and use of the Gravun Service between **Gravun Inc. (“Gravun”)** and the business identified as Customer in that agreement (“**Customer**”).

The applicable Terms of Service, any executed Master Services Agreement, Order Forms, and incorporated contractual documents are together referred to as the “**Agreement.**”

1. Scope and Definitions

1.1 Application. This DPA applies where Gravun processes personal information on Customer’s behalf in providing the Service. It remains effective for as long as Gravun or its Subprocessors retain that information.

1.2 Customer Personal Information. “**Customer Personal Information**” means personal information contained in Customer Content or otherwise collected or generated by the Service on Customer’s behalf, including information about Customer personnel, clients, prospective clients, signers, callers, and message recipients.

1.3 Applicable Privacy Law. “**Applicable Privacy Law**” means privacy, data protection, and data security legislation applicable to the particular processing under the Agreement. Depending on the circumstances, this may include Canadian federal or provincial legislation and applicable United States state privacy legislation. Reference to a law does not make it applicable where its jurisdictional or substantive requirements are not met.

1.4 Processing. “**Processing**” includes collection, recording, organization, storage, access, use, transmission, disclosure, correction, retrieval, restriction, and deletion.

1.5 Subprocessor. “**Subprocessor**” means a third party engaged by Gravun to process Customer Personal Information on Gravun’s behalf in delivering the Service. Gravun personnel acting under its direct authority are not separate Subprocessors.

1.6 Security Incident. “**Security Incident**” means a breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Personal Information within Gravun’s or its Subprocessors’ responsibility.

Unsuccessful attempts that do not compromise Customer Personal Information are not, by themselves, Security Incidents. This exclusion does not narrow an incident definition or notification obligation imposed by Applicable Privacy Law.

1.7 Processing Particulars. Schedule 1 describes the subject matter, purposes, nature, duration, individuals, and information covered by the processing.

2. Roles and Instructions

2.1 Respective Roles. Customer determines the purposes of processing undertaken on its behalf. Gravun acts as Customer's processor, service provider, or equivalent service intermediary, as applicable. Where Customer itself acts for another organization, Customer must hold the authority necessary to appoint Gravun and issue the relevant instructions.

2.2 Documented Instructions. Customer instructs Gravun to process Customer Personal Information as reasonably necessary to provide the purchased Service, operate enabled features, follow authorized workspace settings, and perform the Agreement. Additional instructions must be lawful, documented, and within the agreed scope.

2.3 Operational Authority. Gravun may rely on instructions submitted by Customer's authorized representatives or through appropriately permissioned accounts, subject to the account-authority and security provisions of the Agreement.

2.4 Instructions Outside Scope. An instruction requiring a new service, material technical change, or additional processing arrangement is subject to written agreement on feasibility, scope, and any additional fees. Gravun will not charge separately for an obligation already included in the Agreement or imposed directly on it by law.

2.5 Unlawful Instructions. If Gravun reasonably believes an instruction violates Applicable Privacy Law, it will inform Customer unless legally prohibited. Gravun may suspend the affected processing while the parties resolve the issue. It is not required to follow an unlawful instruction.

2.6 Legally Required Processing. Where law requires processing outside Customer's instructions, Gravun will notify Customer before that processing where legally permitted and reasonably practicable. Processing and disclosure will be limited to what the requirement justifies.

2.7 Independent Activities. This DPA does not govern information that Gravun independently processes for its own subscription administration, billing, business contacts, or other separately established lawful purposes described in its Privacy Policy. Gravun may not avoid this DPA by relabelling Customer Personal Information as account, diagnostic, or business information.

3. Customer Responsibilities

3.1 Lawful Collection and Disclosure. Customer is responsible for establishing the lawful authority to collect Customer Personal Information, provide it to Gravun, and instruct the processing described in this DPA.

3.2 Notices and Permissions. Customer will provide required notices and obtain required permissions for its activities, including communications, recording, transcription, electronic signatures, AI processing, and authorized disclosures to connected services.

3.3 Appropriate Content. Customer will limit information submitted to what is reasonably necessary for its intended use. It will not introduce prohibited information or a processing activity requiring additional safeguards or contractual arrangements without first agreeing those arrangements with Gravun.

3.4 Account Controls. Customer is responsible for its user permissions, access reviews, account credentials, selected integrations, and available workspace retention settings. These responsibilities do not reduce Gravun's own security obligations.

3.5 Accuracy and Requests. Customer determines the accuracy of its business records and the substantive response to requests concerning information under its control, with Gravun's assistance under this DPA.

3.6 No Transfer of Statutory Responsibility. Neither party transfers an obligation imposed directly on it by Applicable Privacy Law merely by allocating operational tasks to the other.

4. Processing Restrictions

4.1 Limited Purposes. Gravun will process Customer Personal Information only for the specified service purposes, documented lawful instructions, and processing otherwise required or expressly permitted by Applicable Privacy Law consistently with this DPA.

4.2 No Sale or Advertising Use. Gravun will not sell Customer Personal Information, share it for cross-context behavioural advertising, or use it for Gravun's own targeted advertising. Customer-directed campaigns within Customer's own business relationship are distinct from such prohibited uses.

4.3 No Unrelated Profiling. Gravun will not use Customer Personal Information to build unrelated commercial profiles of individuals or enrich another customer's records.

4.4 AI Training. Gravun will not use Customer Personal Information, or authorize a Subprocessor to use it, to train general-purpose AI models without a separate written arrangement and all permissions required by law and the source of the information. Ordinary acceptance of this DPA or activation of an AI feature does not provide that authorization. Any additional arrangement must preserve applicable service-provider restrictions.

4.5 Aggregation and De-Identification. Gravun may create and use aggregated or de-identified information only where permitted by the Agreement, Applicable Privacy Law, and source restrictions. Removing a name, replacing an identifier, or hashing a record does not automatically make information anonymous.

Where Gravun relies on de-identified status, it will maintain the safeguards, commitments, and recipient restrictions required by law and will not attempt to re-identify individuals except for legally permitted validation of the de-identification process.

4.6 Connected-Service Restrictions. Additional restrictions applying to information obtained through Google, Microsoft, or another source continue to apply. A Customer instruction cannot authorize Gravun to disregard those restrictions.

5. Confidentiality and Security

5.1 Personnel. Gravun will restrict personnel access to those who need it for authorized duties. Persons permitted to process Customer Personal Information must be subject to appropriate confidentiality obligations and receive instructions relevant to their responsibilities.

5.2 Safeguards. Gravun will maintain administrative, technical, and organizational measures appropriate to the nature and sensitivity of the information and the risks of processing, including the measures in Schedule 2.

5.3 Security Changes. Gravun may update its security measures as technology and risks change, provided the changes do not materially reduce the overall protection promised under the Agreement.

5.4 Shared Responsibility. Customer remains responsible for safeguards within its control, including its devices, networks, user administration, and instructions. Gravun remains responsible for the security measures allocated to it.

5.5 No Implied Certification. This DPA does not represent that Gravun holds a particular certification, independent assurance report, or recovery capability unless expressly identified in an incorporated schedule.

6. Subprocessors

6.1 Authorization. Customer grants general authorization for Gravun to engage the Subprocessors identified in the completed Schedule 3 and additional Subprocessors appointed under this Section. Authorization is limited to the processing necessary for their stated functions.

6.2 Selection and Contracts. Before providing access, Gravun will assess the Subprocessor's suitability and enter into a written agreement imposing protections appropriate to its processing and no less protective in substance than the applicable obligations of this DPA.

6.3 Continuing Responsibility. Gravun remains responsible to Customer for its Subprocessors' performance of the obligations subcontracted to them, subject to the Agreement's liability provisions.

6.4 Advance Notice. Gravun will give at least thirty (30) days' notice before a new or replacement Subprocessor begins processing Customer Personal Information. Notice will identify the provider, its function, relevant processing locations, and the affected service. Customer must maintain a current notification address.

6.5 Objections. Customer may object within fifteen (15) days of notice on reasonable, documented data protection grounds. The parties will seek a proportionate

resolution, which may include an alternative configuration, additional safeguards, or discontinuation of the affected optional feature.

6.6 Unresolved Objection. If no reasonable solution is available before the proposed processing begins, either party may terminate the affected service by written notice. Gravun will refund prepaid fees attributable to the unused terminated portion. Unaffected services remain in force.

6.7 Urgent Replacement. Where immediate replacement is reasonably necessary to address a serious security issue, unexpected provider cessation, or legal requirement, Gravun may appoint a replacement on shorter notice if lawful. It will notify Customer as soon as practicable, explain the urgency, and preserve Customer's objection and affected-service termination rights.

6.8 Customer-Selected Providers. A provider separately selected and contracted by Customer is not Gravun's Subprocessor merely because Customer connects it to the Service. Classification depends on the actual processing relationship. Gravun remains responsible for its own authorized transmission to that provider and may not classify its own outsourced processing as a Customer integration to avoid this Section.

7. International Processing

7.1 Locations. Customer authorizes processing in the locations identified in the completed schedules, subject to Applicable Privacy Law and any express location restriction in the Agreement.

7.2 Canadian Hosting. The location of the core database does not, by itself, restrict every communication route, support activity, AI operation, or Subprocessor to Canada.

7.3 Transfer Requirements. Each party will perform the transfer assessments and contractual measures allocated to it by Applicable Privacy Law. Gravun will provide reasonably available information required for Customer's assessment of an intended transfer.

7.4 Location Changes. Gravun will notify Customer before a material change to a disclosed processing location. Where the change raises reasonable data protection concerns, the objection and resolution process in Section 6 applies.

7.5 Additional Jurisdictions. This DPA does not incorporate European Union or United Kingdom standard contractual clauses by implication. If processing requires a transfer mechanism not already in place, the parties must execute the necessary instrument before the affected transfer.

8. Requests, Assessments, and Regulatory Assistance

8.1 Individual Requests. Gravun will promptly notify Customer of a request concerning Customer Personal Information received directly from an individual, unless prohibited by law. Gravun may acknowledge receipt and identify Customer as the responsible organization but will not decide the substantive response unless authorized or legally required.

8.2 Assistance. Taking account of the processing and information available to it, Gravun will reasonably assist Customer with access, correction, deletion, portability, restriction, consent withdrawal, and other applicable rights.

8.3 Response Periods. Assistance will be provided without undue delay and with reasonable regard to Customer's notified statutory deadline. Customer must submit sufficiently specific instructions and promptly provide information needed to locate the relevant records.

8.4 Assessments. Gravun will reasonably assist with privacy impact assessments, data protection assessments, and consultations with authorities where required for processing under this DPA.

8.5 Charges. Standard functionality and assistance required to remedy Gravun's breach are included. For unusually extensive assistance outside existing contractual or legal obligations, the parties may agree reasonable fees in advance. A fee dispute will not justify withholding assistance that Gravun is legally required to provide within a fixed deadline.

9. Security Incidents

9.1 Notification. Gravun will notify Customer without undue delay after becoming aware of a Security Incident affecting Customer Personal Information, and within any shorter period required by Applicable Privacy Law. Gravun will not postpone initial notice solely because its investigation is incomplete.

9.2 Initial Information. To the extent known, notice will describe the nature of the incident, affected information and individuals, likely consequences, containment or corrective measures, and a contact for further enquiries. Missing information may be supplied in stages.

9.3 Response. Gravun will promptly investigate, take reasonable steps to contain and remediate the incident, preserve relevant evidence, and cooperate with Customer concerning obligations arising from it.

9.4 External Notices. Customer determines notifications concerning information under its control, except where law imposes a direct obligation on Gravun. Where legally permitted and practicable, the parties will coordinate notices to avoid inconsistent or misleading statements. Neither party may prevent a notice required by law.

9.5 Scope of Disclosure. Assistance does not require disclosure of another customer's information, privileged material, or details whose disclosure would create a material security risk. Gravun will provide an appropriate summary or alternative evidence where possible.

9.6 No Admission. Providing notice or assistance is not an admission of fault. Responsibility for losses and response costs is governed by the Agreement and Applicable Privacy Law.

10. Compliance Information and Audits

10.1 Information. Gravun will make available information reasonably necessary to demonstrate compliance with this DPA.

10.2 Review Process. The parties will ordinarily begin with available documentation, questionnaires, and relevant independent assessments, where available. Customer may request a further assessment where that material is insufficient to meet a reasonable compliance need.

10.3 Audit Rights. Customer, or an independent auditor acting under confidentiality obligations, may conduct a reasonable assessment of the processing covered by this DPA. Where Applicable Privacy Law permits, Gravun may provide a qualifying independent assessment and report instead.

10.4 Safeguards. Routine audits require reasonable advance notice, a defined scope, and arrangements minimizing disruption. Auditors must not be direct competitors of Gravun and may not access another customer's data or conduct intrusive technical testing without an agreed protocol.

10.5 Frequency and Exceptions. Routine audits are ordinarily limited to once in twelve months. Additional assessments may be conducted where required by law or an authority, following a material Security Incident, or where credible evidence indicates material non-compliance. Contractual procedures will not obstruct a legally required assessment.

10.6 Costs and Remediation. Customer bears its own routine audit costs. Gravun bears the cost of correcting its established non-compliance. Any additional charges for assistance must be reasonable and agreed in advance, and must not impair mandatory oversight rights.

11. Return, Retention, and Deletion

11.1 Customer Choice. On cessation of the relevant services, Gravun will, at Customer's choice, return or delete Customer Personal Information, subject to the export period in the Agreement and lawful retention requirements.

11.2 Standard Export Period. Unless otherwise agreed, Customer has thirty (30) days after termination to obtain the available export. Unless Customer gives a different lawful instruction, expiry of that period constitutes an instruction to delete under the deletion timetable in Schedule 1.

11.3 Retained Copies. Information may remain in protected backups until the stated backup cycle expires or where retention is required by law. Retained information remains protected and is not used for unrelated purposes. Deletion instructions will be reapplied if a backup is restored.

11.4 Signing Records. Signed documents, certificates, consent evidence, and audit records must be considered separately when assessing deletion. Gravun will not assume that deleting a signer profile removes the individual's information from those records. Nor will it assume that every signing record must be retained indefinitely.

11.5 Legal Holds. Where retention is legally required, Gravun will limit it to the relevant information and period and inform Customer where permitted. Retention for another claimed legal exception must be permitted by Applicable Privacy Law and documented; a general interest in preserving all records is insufficient.

11.6 Subprocessors and Confirmation. Gravun will instruct relevant Subprocessors to return or delete information consistently with this DPA. On reasonable request, it will provide written confirmation of completed deletion, identifying any remaining lawful retention or backup expiry period.

11.7 External Copies. These duties apply to information within Gravun's and its Subprocessors' responsibility. They do not require Gravun to delete copies independently held by Customer, document recipients, or Customer-selected providers.

12. Jurisdiction-Specific Requirements

12.1 Canadian Processing. Where Canadian privacy legislation applies, Gravun will protect Customer Personal Information transferred to it for processing through the safeguards and contractual measures in this DPA. Customer's continuing accountability does not relieve Gravun of its own duties.

12.2 Québec Service Arrangements. Where Québec private-sector privacy law applies, Gravun will use the information only to perform the mandate or contract, maintain appropriate confidentiality protections, and refrain from retaining it after completion except where legally permitted or required. Gravun will notify Customer's designated privacy officer without delay of a violation or attempted violation by any person of an obligation concerning the confidentiality of the information. Customer may verify compliance in accordance with Section 10, without restricting any broader mandatory verification right.

12.3 United States Processor Obligations. Where an applicable United States state privacy law treats Gravun as a processor, Gravun will follow Customer's lawful instructions, impose personnel confidentiality duties, provide required assistance, support reasonable assessments, and bind Subprocessors to applicable protections.

12.4 California Restrictions. Where Gravun receives personal information as a service provider or contractor under the California Consumer Privacy Act, as amended, Gravun will:

- (a) process it only for the limited and specified purposes in Schedule 1;
- (b) not sell or share it as those terms are defined by that law;
- (c) not retain, use, or disclose it outside the direct business relationship with Customer or for another commercial purpose, except as expressly permitted by that law;
- (d) not combine it with information obtained from another person or from Gravun's own interactions with an individual, except to the extent expressly permitted by that law and consistently with this DPA; and

(e) provide the same level of privacy protection required by applicable California law.

12.5 California Oversight. Customer may take reasonable and appropriate steps to verify that Gravun uses the information consistently with applicable California obligations and, on notice, to stop and remediate unauthorized use. Gravun will notify Customer if it determines that it can no longer meet those obligations.

12.6 Certification. By accepting this DPA, Gravun certifies that it understands and will comply with the restrictions in Sections 12.4 and 12.5 where applicable.

13. Priority, Liability, and Execution

13.1 Priority. This DPA prevails over conflicting provisions concerning the processing and protection of Customer Personal Information. Mandatory legal requirements prevail over inconsistent contractual provisions.

13.2 Liability. The limitations, enhanced caps, exclusions, and indemnity procedures in the Agreement apply to this DPA. This DPA does not create a separate indemnity, duplicate liability limit, or additional category of unlimited liability. Contractual limits do not restrict an authority's powers or an individual's non-waivable statutory rights.

13.3 Changes. Amendments require the method specified in the Agreement, except for Subprocessor updates made under Section 6. No schedule update may expand permitted purposes or materially reduce protection by implication.

13.4 Acceptance. This DPA becomes binding when incorporated into an accepted Agreement or executed below. Separate signatures are unnecessary where the Agreement already validly incorporates this DPA.

For Gravun Inc.

Signature: _____

Name: Ahmed Radi

Title: Founder

Date: [Insert]

For Customer

Signature: _____

Name: [Insert]

Title: [Insert]

Date: [Insert]

SCHEDULE 1**PROCESSING PARTICULARS****1.1 Subject Matter and Duration**

Processing supports Customer's use of Gravun's business-management platform during the subscription and the limited return, deletion, and lawful retention periods following it.

1.2 Nature and Specified Purposes

Processing activity	Specified purpose
Collection, organization, storage, and retrieval	Maintain Customer's contact, job, appointment, and business records
Document and transaction processing	Prepare and manage estimates, invoices, work orders, and payment-status records
Communication routing and recording	Deliver Customer-authorized email, SMS, calls, recordings, transcripts, and associated records
Electronic signing	Present documents and consent, collect signatures, generate completed documents and certificates, and maintain signing evidence
AI processing	Provide enabled receptionist, drafting, summarization, and authorized workflow functions
Integrations and imports	Exchange information with services authorized by Customer
Technical and support processing	Apply permissions, investigate errors, protect the Service, and answer authorized support requests
Export, correction, and deletion	Carry out lawful Customer instructions and assist with applicable privacy obligations

The scope is limited to purchased or enabled features. Listing a function does not authorize unrelated processing.

1.3 Individuals

Customer personnel and contractors; prospective and existing clients; homeowners and business contacts; suppliers; document signers; callers; message recipients; and individuals identified in Customer-provided records.

1.4 Information Categories

Names, business details, contact information, service addresses, appointment and job records, financial transaction records, communications, recordings, transcripts, uploaded materials, signatures, consent records, document fingerprints, IP addresses, device information, timestamps, access records, and relevant integration data.

Sensitive information is included only to the extent lawfully submitted and permitted under the Agreement. This schedule does not authorize biometric identification, regulated health-data processing, or another specialized use merely because a recording or document could contain relevant information.

1.5 Processing Frequency

Continuous or event-driven during use of the relevant feature.

1.6 Retention and Deletion Parameters

Parameter	Agreed arrangement
Active subscription retention	Customer's lawful instructions and agreed category-specific retention settings
Post-termination export period	30 days unless expressly varied
Deadline for deletion from active systems after export period or valid deletion instruction	[Insert verified operational period]
Maximum backup expiry period	[Insert verified period]
Provider-specific residual retention	[Identify applicable periods and exceptions]
Legal retention	Limited to the information and period justified under Section 11
Signing-record arrangements	[Identify agreed retention instructions or applicable policy version]

1.7 Contacts

Function	Gravun	Customer
Privacy and instructions	Ahmed Radi	[Name or role and monitored email]
Security incidents	Hello@gravun.com	[Monitored email]
Subprocessor notices	Hello@gravun.com	[Notification email]

SCHEDULE 2

SECURITY REQUIREMENTS

The following are contractual requirements for processing under this DPA. They are not a representation of independent certification.

2.1 Access Management. Access must be limited according to role and operational need, with procedures for granting, reviewing, and revoking access. Privileged access must receive protection appropriate to its risk.

2.2 Workspace Separation. Appropriate logical controls must restrict access between Customer workspaces and prevent unauthorized cross-workspace disclosure.

2.3 Information Transmission and Storage. Customer Personal Information must be protected during transmission and storage using measures appropriate to its sensitivity. Encryption, credentials, secrets, and access tokens must be managed securely.

2.4 System Maintenance. Gravun must maintain procedures for identifying and addressing relevant vulnerabilities, applying security updates, and controlling material changes to production systems.

2.5 Logging. Relevant access, administrative, and security events must be recorded and protected against unauthorized alteration. Logs must avoid unnecessary collection of message content, credentials, or other sensitive information.

2.6 Recovery. Backup and restoration arrangements must be maintained and reviewed according to the service's needs. Any specific recovery-time or recovery-point commitment must be separately agreed.

2.7 Incident Handling. Gravun must maintain procedures for reporting, assessing, containing, investigating, and documenting Security Incidents and coordinating required notifications.

2.8 Personnel and Providers. Personnel must receive appropriate confidentiality and security instructions. Providers with access must be assessed and contractually bound under Section 6.

2.9 Disposal. Deletion, disposal, and backup expiry must be managed to prevent unauthorized recovery or continued unrelated use, subject to lawful retention.

2.10 Customer Configuration. Customer must manage its users, permissions, devices, sharing decisions, and integration credentials and promptly report suspected compromise.

SCHEDULE 3 — SUBPROCESSORS AND CONNECTED PROVIDERS

Last Verified: September 18, 2026

3.1 Interpretation

The register below reflects the providers identified for Gravun’s architecture. Before this schedule is used for contractual authorization, Gravun must complete the contracting entities, relevant processing countries, and deployed-service details. A brand name does not identify the contracting entity or prove a particular processing location.

Only providers used for the purchased or enabled functions receive the relevant information.

3.2 Providers Processing on Gravun’s Behalf

Provider / contracting entity	Function	Relevant information	Processing location and deployment particulars
Supabase — [Confirm entity]	Database, storage, and authentication	Workspace records, files, account and authentication information	Core project: Canada Central; confirm backup, support, and other processing locations
Twilio — [Confirm entity]	SMS, telephony, and associated recording services	Telephone numbers, message content, call data, recordings, delivery records	[Confirm countries and services used]
Vapi — [Confirm entity]	AI voice orchestration	Audio, transcripts, call metadata, relevant instructions and context	[Confirm countries and downstream- provider routing]
Deepgram — [Confirm entity]	Speech transcription	Audio and resulting transcripts and metadata	[Confirm countries and retention settings]
Anthropic — [Confirm entity]	Primary AI model services	Relevant prompts, workspace context, and outputs	[Confirm countries, account terms, and retention settings]
OpenAI — [Confirm entity]	Optional AI model services	Relevant prompts, workspace context, and outputs	[Confirm whether enabled, countries, and retention settings]
Resend — [Confirm entity]	Email delivery	Recipient details, email content,	[Confirm deployment and

entity]		attachments where used, delivery records	countries]
Postmark — [Confirm entity]	Email delivery	Recipient details, email content, attachments where used, delivery records	[Confirm deployment and countries]
Sentry — [Confirm entity]	Error and performance diagnostics	Technical events, identifiers, and diagnostic data remaining after configured filtering	[Confirm region, filtering, and retention]

3.3 Providers Requiring Role-Specific Classification

Provider	Function	Classification to record
Stripe — [Confirm entity]	Subscription or Customer payment processing	Identify activities undertaken as processor/service provider and activities governed by Stripe's independent legal or payment obligations
Google Maps — [Confirm entity]	Address lookup or geocoding	Confirm API, transmitted fields, and applicable provider role; include in Section 3.2 where it processes on Gravun's behalf
Web Push provider or infrastructure — [Identify]	Browser notifications	Identify provider, payload contents, role, and processing locations
Other hosting or deployment infrastructure — [Identify]	Application hosting or related operations	Identify any additional provider receiving Customer Personal Information

A provider's independent role does not remove Gravun's responsibility for lawfully disclosing information to it.

3.4 Customer-Authorized Connections

Connection	Authorized activity	Scope limitation
Google Gmail and Calendar	Email and calendar functionality	Limited to granted permissions and applicable

		Google data-use restrictions
Microsoft Outlook and Calendar	Email and calendar functionality	Limited to granted permissions and applicable Microsoft requirements
HubSpot	Authorized CRM import	Limited to the configured import and permitted records
External AI or MCP connection selected by Customer	Authorized access or actions through the connection	Limited to the expressly granted workspace permissions

These are not automatically Gravun Subprocessors. Their status must reflect who appoints the provider and the actual processing arrangement.

3.5 Excluded Infrastructure

A provider used only for Gravun’s corporate website, source-code storage, or internal business operations is not included as a Customer-data Subprocessor unless it actually receives Customer Personal Information. If deployment, logging, support, or another workflow gives it such access, it must be assessed and added before that processing begins.

3.6 Maintaining the Register

Gravun will maintain accurate information about authorized Subprocessors, functions, and processing locations and apply Section 6 to relevant changes. A provider’s own downstream processors remain subject to the applicable contractual chain and oversight requirements.