



# CGS GLOBAL

*Creative Guest Solutions Global*

## Master Terms, Data, Privacy, and Operating Policy

---

<b>Version</b>	2.0 — May 2026
<b>Replaces</b>	All prior CGS data and privacy documents
<b>Applies to</b>	All CGS services, products, tools, team members, and engagements
<b>Contact</b>	operations@cgsglobal.net   619-949-2202   cgsglobal.net
<b>Jurisdiction</b>	State of California, USA

## 1. Who CGS Is and What We Do

---

CGS Global is a business intelligence company.

We observe. We read. We diagnose. We apply human logic to data, patterns, and technology tools to produce intelligence that helps businesses understand what is actually happening in their operations.

CGS is itself a tool, an instrument of observation and analysis in the hands of the people who engage us. We do not guarantee outcomes. We do not predict the future. We read what exists at the moment of observation and return a diagnosis built from what we find.

Reality and patterns cannot be predicted with certainty. What CGS observes today may change tomorrow. We are not liable for reality itself, for what exists, what is missing, what changes, or what outcomes follow from decisions made on the basis of our work.

This policy governs how CGS operates, what we do with data, and what every person who engages with us can expect.

## 2. The Intelligence Doctrine

---

Everything CGS does produces intelligence. Every session, every engagement, every diagnosis teaches CGS something about how businesses operate in the real world. That learning is CGS property.

### What this means in practice:

- CGS records sessions, observes patterns, and synthesizes what it finds across engagements.
- Client identity is never disclosed in any cross-engagement use of intelligence.
- Patterns, rhythms, and operational observations, stripped of identifying information, are used to develop, refine, and improve CGS's methodology and products.
- By engaging with CGS in any capacity, as a managed client, an Intelligence Find session client, a Clarity Session participant, or a pipeline contact, you consent to your anonymized operational patterns being used for CGS methodology development.
- This is the exchange: your reality, anonymized, helps build something that helps the next person.

### What this does not mean:

- CGS does not sell, license, or trade your identifying information to any third party.
- CGS does not disclose your business situation, financials, or strategy to any other client.
- CGS does not use your data to benefit a competitor.
- Your anonymized patterns are used for intelligence development only, not for marketing, advertising, or external commercial purposes.

## 3. CGS Methodology — Proprietary IP

---

The sequences, frameworks, diagnostic logic, and analytical methods CGS uses to produce its outputs are proprietary intellectual property belonging exclusively to CGS Global.

- Clients receive outputs, diagnoses, analyses, recommendations, and deliverables.
- Clients do not receive, and are not entitled to, the underlying methodology that produced those outputs.
- No engagement, contract, or payment transfers CGS methodology, frameworks, or diagnostic sequences to any client under any circumstances.
- CGS methodology is not disclosed, described in operational detail, or reproduced in any client-facing document.
- The fact that CGS uses AI tools, human logic, and pattern recognition in combination is disclosed. The specific sequences and logic CGS applies are not.

This protection applies permanently. It does not expire at engagement end. It is not waived by silence, familiarity, or length of relationship.

## 4. Limits of Liability — What CGS Is and Is Not Responsible For

---

CGS diagnoses what exists at the moment of observation.

Incomplete data produces incomplete diagnoses.

Inaccurate data produces inaccurate diagnoses.

Withheld data produces limited diagnoses.

The quality of the input is the client's responsibility.

The quality of the observation is CGS's.

### **CGS is not liable for:**

- Business decisions made on the basis of CGS diagnoses or recommendations.
- Outcomes that follow from acting or failing to act on CGS intelligence.
- Diagnoses that reflect incomplete, inaccurate, or withheld information provided by or on behalf of the client.
- Changes in business reality that occur after the observation was made.
- Patterns that shift, reverse, or evolve after diagnosis.
- The accuracy or reliability of outputs produced by third-party AI tools, technology platforms, or processors used in CGS's work.
- Breaches, failures, or data incidents originating within third-party platform infrastructure.
- The conduct of clients within their own systems and environments.

### **CGS is liable for:**

- The quality and professionalism of its observations within the scope of access granted.
- The conduct of its team members inside client environments.
- Operating within the scope of access authorized by the client.
- Responding appropriately to data incidents within CGS's systems and control.

CGS's maximum liability for any claim arising from any engagement is limited to the fees paid by the client for the specific service from which the claim arises. CGS is not liable for indirect, consequential, incidental, or punitive damages of any kind.

## 5. Tools, Technology, and AI

---

CGS uses multiple technology tools at all times in the delivery of its services. These tools include AI platforms, CRM systems, meeting transcription tools, cloud storage, and

communication platforms. Tools change. New tools are added. The list below reflects current operations and is updated when material changes occur.

**Current tools in active use:**

- Google Workspace — document storage, collaboration, client shared drives
- Fathom — meeting recording and transcription
- GoHighLevel (GHL) — CRM, pipeline management, client sub-accounts, outreach automation
- WhatsApp — client and team operational communication
- AI tools including Anthropic Claude and others — diagnostic synthesis, content development, pattern analysis

**How CGS uses tools:**

- Tools are instruments. CGS applies human logic to tool outputs. No tool operates autonomously on behalf of CGS or its clients without human review.
- CGS specializes in human logic applied to technology — not the reverse. The tool serves the thinking. The thinking is never delegated to the tool.
- No output produced by any tool, including AI, is delivered to a client without CGS professional review.

**AI tools — specific disclosure:**

- CGS uses AI tools in diagnostic and analytical work. AI tools process CGS observations and language derived from engagement activity.
- CGS does not submit raw client data files directly to AI platforms.
- Data processed through AI tools is governed by those tools' published terms of service and privacy policies in addition to this policy.
- No AI tool used by CGS is permitted by its own terms to use customer conversation data to train AI models. CGS operates in compliance with those terms.
- CGS is responsible for what it submits to AI tools and what it delivers from them. The AI platforms are responsible for their own infrastructure, security, and data handling practices.

**No output guarantee:**

No output produced by CGS, its tools, its team, or any combination thereof constitutes a guarantee of business results, accuracy, or fitness for any specific purpose. Intelligence is observational. It reflects what exists at the time of observation. It does not predict, guarantee, or warrant any outcome.

## 6. How CGS Operates — The Three Access Modes

---

CGS operates in three distinct modes depending on the service. Each mode has a different liability profile and different data handling requirements. All three are disclosed here.

### 6.1 Shared Drive — Client-Owned Environment

The client creates or shares a Google Drive with CGS. The client owns the drive. CGS has granted access to operate within it. CGS creates deliverables — task sheets, analyses, summaries — inside the client's environment. The data belongs to the client. CGS is an authorized accessor, not a data custodian.

### 6.2 Remote Access — Client Systems

The client grants CGS access to their own systems — inbox, calendar, CRM, booking systems, financial platforms. The client holds the credentials. CGS operates inside the client's live environment as an authorized user. CGS never holds client credentials in CGS systems. Access is granted by the client and can be revoked at any time. CGS is responsible for its conduct within that access. The client is responsible for the security of their own environment.

### 6.3 GHL Sub-Accounts — CGS-Administered Systems

CGS builds and administers GoHighLevel sub-accounts for clients within CGS's GHL agency master account. The client's full operational data — contacts, leads, conversations, automations, booking data — lives in the sub-account. The client accesses and uses the sub-account directly. CGS holds master-level administrative access above the client's access.

#### What this means for client data in GHL sub-accounts:

- CGS is the system administrator. GHL is the platform infrastructure provider. The client is the data controller of their own business data.
- The client's leads and customers whose information is in the sub-account did not consent directly to CGS. They consented to the client's business. CGS operates as a data processor on behalf of the client as data controller.
- The client is responsible for ensuring that their collection and use of their customers' data in the sub-account complies with applicable law.
- GHL's platform-level security, compliance, and data practices are governed by GHL's published terms and privacy policy. GHL maintains SOC 2 Type II, CCPA, and GDPR compliance at the platform level.
- At engagement termination, CGS provides the client with their sub-account data export within 30 days of request. Sub-account data is not retained by CGS beyond the retention period specified in Section 8.

## 7. Operator Access and Conduct

---

CGS delivers services through a team of operators — contractors who access client environments and execute assigned tasks. All operators are bound by the CGS Operator Confidentiality Agreement before any access is granted.

### **Operator standards — non-negotiable:**

- Access is scoped to the assigned client only. No operator has standing access to other client environments.
- Operators do not extract, screenshot, copy, or transmit client data to any system outside the approved CGS platform environment.
- Operators do not discuss one client's situation, data, or engagement with any other client or unauthorized party.
- Operators do not submit raw client data to any AI tool without principal authorization.
- Operators do not make commitments or representations to clients without CGS principal authorization.
- Operators report any data incident to the CGS principal on the same business day it is identified.
- Upon engagement termination, operators confirm deletion of locally held client data within 5 business days.

CGS is responsible for operator conduct with respect to client data. Operator access is logged and scoped. If an operator causes a data incident, CGS's obligation to its clients may require disclosure of the operator's identity. Operators acknowledge this in their confidentiality agreement.

## 8. Data Retention and Deletion

CGS retains data for the minimum period necessary for legal compliance and operational reference. Records are deleted — not archived — upon expiry. Deletion is confirmed and logged annually.

Record Type	Retention	Action at Expiry
Signed MSAs, SOWs, and agreements	7 years	Delete — confirm in deletion log
Client Disclosure Statements	7 years	Delete — confirm in deletion log
Operator Confidentiality Agreements	7 years	Delete — confirm in deletion log
Billing and payment records	7 years	Delete — confirm in deletion log
Fathom meeting summaries	3 years	Delete — confirm in deletion log
Client deliverables and analyses	3 years or client request	Delete — confirm in deletion log
GHL sub-account data post-termination	1 year post-engagement	Export to client on request; delete
GHL contact records (pipeline)	1 year post-engagement	Archive or delete from GHL
Intelligence Find session logs	3 years	Delete — confirm in deletion log
Intelligence Find agreements	7 years	Delete — confirm in deletion log
Intelligence Find diagnostic outputs	3 years or client request	Delete — confirm in deletion log
Clarity Session contact records	1 year from session date	Delete from GHL and Drive
Clarity Session Fathom summaries	1 year from session date	Delete — confirm in deletion log
Team payroll and time records	7 years	Delete — confirm in deletion log
Internal weekly intelligence documents	2 years	Archive in internal folder
Anonymized methodology intelligence	Indefinite	Retained as CGS proprietary IP — no expiry

## 9. Your Rights

---

Any person or business whose data CGS holds has the following rights. To exercise any of these rights, contact [operations@cgsglobal.net](mailto:operations@cgsglobal.net). CGS responds within 10 business days.

- Know — request a description of what categories of data CGS holds about you.
- Access — request a copy of your data held in CGS systems.
- Correct — request correction of inaccurate data.
- Delete — request deletion of your data subject to legally required retention periods.
- Portability — request your data in a portable format.
- Opt out of recording — request that Fathom not record calls involving you. CGS will accommodate this request for any scheduled session.
- Object — object to specific data processing activities. CGS will assess and respond within 10 business days.

California residents have additional rights under CCPA and CPRA. CGS does not sell personal information. CGS does not use personal information for cross-context behavioral advertising. California residents may exercise all rights listed above by contacting [operations@cgsglobal.net](mailto:operations@cgsglobal.net).

## 10. Breach Response

---

Speed and transparency are the primary protections — not concealment. If something goes wrong, CGS moves fast and speaks plainly.

### **Detection — immediate**

Any CGS team member who identifies or suspects a data incident — unauthorized access, data loss, accidental disclosure, or anomalous system behavior — reports to the CGS principal immediately via direct message and phone on the same business day.

### **Assessment — within 4 hours**

The CGS principal assesses what data was involved, how many individuals or clients are affected, whether the incident is confirmed or suspected, and whether legal counsel should be engaged.

### **Notification — within 48 hours of confirmation**

Affected clients are notified directly by the CGS principal. Notification is plain language: what occurred, what data was involved, what steps CGS is taking. No delay. No minimization.

### **Regulatory notification**

If the breach involves Personal Information of California residents and meets the threshold for mandatory notification under California law, CGS notifies the California Attorney General as required and consults legal counsel.

### **Documentation**

Every incident is documented in full in the CGS internal folder with: incident description, timeline, data involved, affected parties, notifications sent, and remediation steps taken. Retained for 7 years.

## **11. Governing Law**

---

This policy and all CGS data handling practices are governed by the laws of the State of California. CGS acknowledges its obligations under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA). Any dispute arising under this policy shall be resolved in San Diego County, California.

## **12. How to Find This Policy**

---

This policy is publicly available.

It is linked from every CGS client-facing document. It is linked from the CGS website.

It is referenced in every MSA, SOW, and engagement agreement. It is provided to every operator before access is granted.

It is provided to every client before engagement begins.

**If you engaged with CGS and were not aware of this policy, it is because you did not look — not because CGS did not disclose it.**

CGS informs. Always.

Direct link: [cgsglobal.net/privacy](https://cgsglobal.net/privacy) | Available on request: [operations@cgsglobal.net](mailto:operations@cgsglobal.net)

## 13. Policy Updates

---

This policy replaces all prior CGS data, privacy, and confidentiality documents. It is reviewed annually and updated whenever material operational changes occur. Material updates are communicated to active clients with 30 days notice. Continued engagement with CGS following notice constitutes acceptance of the updated policy.

Current version: 2.0 — May 2026. Next scheduled review: May 2027.

Policy owned by: CGS Principal. COO responsible for operator compliance.

---

CGS Global | [operations@cgsglobal.net](mailto:operations@cgsglobal.net) | 619-949-2202 | [cgsglobal.net](https://cgsglobal.net)

*Version 2.0 — May 2026 — This policy supersedes all prior versions*

**Copyright CGS©2026**