DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement ("**Agreement**") is entered into by and between:

Controller: Information owner ("**Controller**")

and

Processor: Gamma Technologies, LLC, a Delaware limited liability company with its registered office at 700 Oakmont Lane, Suite 300, Westmont, Illinois 60559 USA ("**Processor**").

Collectively referred to as the "**Parties**".

---

1. SUBJECT MATTER AND DURATION

1.1. This Agreement governs the Processor's Processing of Personal Data provided by the Controller or employees of the Controller.

1.2. This Agreement shall remain in effect for as long as the Processor Processes Personal Data on behalf of the Controller.

---

2. DEFINITIONS

"**Personal Data**," "**Processing**," "**Controller**," "**Processor**," "**Data Subject**," and "**Supervisory Authority**" shall have the same meanings as set forth in the GDPR.

---

3. SCOPE AND PURPOSE OF PROCESSING

3.1. The Processor shall Process Personal Data only based on the data provided by the Controller and its employees, including any transfer of such data out of its home country.

3.2. The subject matter, nature, and purpose of the Processing, the types of Personal Data, and categories of Data Subjects are described in **Annex I**.

---

4. OBLIGATIONS OF THE PROCESSOR

The Processor shall:

- Process Personal Data only provided by the Controller, including if the Controller provides any specific instructions as to such Processing;
- Ensure persons authorized to Process the Personal Data have committed to confidentiality obligations;
- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR);
- Assist the Controller in responding to Data Subject requests;
- Assist in ensuring compliance with Articles 32 to 36 of the GDPR;
- At the Controller's choice, delete or return all Personal Data after the end of the provision of services;
- Make available all information necessary to demonstrate compliance with this Agreement and allow for audits.

---

5. SUB-PROCESSORS

5.1. The Controller authorizes the use of sub-processors listed in **Annex III**.

5.2. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors by updating this Agreement on the Processor's website; it is incumbent on the Controller to periodically review the Processor's website for any updates. The Controller may object to such changes.

5.3. The Processor shall enter into a written agreement with each sub-processor imposing obligations no less protective than those in this Agreement.

---

6. INTERNATIONAL DATA TRANSFERS

6.1. Where Personal Data is transferred from the European Economic Area (EEA) or United Kingdom to the United States, such transfer shall be governed by the **Standard Contractual Clauses (SCCs)** adopted by the European Commission Decision 2021/914 of 4 June 2021, attached as **Annex IV**.

6.2. Where necessary, the Processor shall implement additional safeguards to ensure the level of protection required under EU law.

---

7. LIABILITY

The Processor shall be liable for the damage caused by Processing only where it has not complied with its obligations under the GDPR or acted with willful misconduct with respect to the lawful instructions of the Controller.

---

8. TERMINATION

Upon termination of the relationship between the Parties hereto or this Agreement, the Processor shall, at the Controller's choice, delete or return all Personal Data, unless Union or Member State law requires storage of the Personal Data.

---

9. GOVERNING LAW

This Agreement shall be governed by the laws of home country of the Controller.

GAMMA
TECHNOLOGIES

ANNEX I – DESCRIPTION OF PROCESSING

- **Nature and purpose of processing:** communication and support
- **Duration:** for the length of the contractual relationship between Controller and Processor, or until such time as the Controller requests deletion of data
- **Categories of Data Subjects:** any party that provides data to the Processor, including but not limited to employees of Controller, job applicants, prospective clients, and GT website registrants
- **Types of Personal Data:** employee names, email addresses, business phone numbers, IP addresses.

ANNEX II – TECHNICAL AND ORGANIZATIONAL MEASURES

1. INFORMATION SECURITY POLICY

   We maintain and adhere to an internal, written Information Security Policy.

2. ACCESS CONTROL

   2.1 Access controls: Network access control mechanisms are designed to prevent traffic using unauthorized protocols from reaching the network infrastructure.

   2.2 Endpoint Hardening: Endpoints are hardened in accordance with industry standard practice. Workstations are protected using anti-malware and endpoint detection & response tools, receiving regular definition and signature updates.

   2.3 Limitations of Privilege and Authorization Requirements - Privileged Access Management: Privileged access in our environment is controlled and monitored. Non-personal accounts used for system access are stored in a secure vault with additional controls governing privilege elevation and account check out processes.

   Product Access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Administrative or high risk access permissions are reviewed annually.

   2.4 Non-Cloud Platform Data: The Processor shall ensure that all sensitive data transferred by the Controller is stored in documented locations within the Processor's internal networks. These locations must be secured using industry-standard encryption methods both at rest and in robust authentication mechanisms and access controls. The Processor shall implement regular security audits and monitoring to detect and respond to any unauthorized access or potential vulnerabilities promptly. Additionally, the Processor shall maintain comprehensive logs of all access and data handling activities to ensure traceability and accountability.

3. TRANSMISSION CONTROL

   In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces internally and GT cloud products. Our HTTPS implementation uses industry standard algorithms and certificates.

   At-rest: We store user passwords following policies that follow industry standard practices for security. We take a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted.

4. INCIDENT MANAGEMENT, LOGGING, AND MONITORING

Incident Response Plan: We maintain a written Incident Response Plan, playbooks, and other necessary processes and procedures to fulfill the standards and obligations reflected therein.

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

5. AVAILABILITY CONTROL

GT SaaS Product infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure high uptime. The providers maintain redundancy to power, network, and heating, ventilation and air conditioning (HVAC) services.

Fault tolerance: Backup strategies are designed to ensure redundancy and fail-over.

Disaster Recovery Plans: We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes.

6. VULNERABILITY MANAGEMENT PROGRAM

Vulnerability Remediation Schedule: We maintain a vulnerability remediation schedule aligned with industry standards. We take a risk-based approach to determining a vulnerability's applicability, likelihood, and impact in our environment.

Vulnerability scanning: We perform regular vulnerability scanning on our products using technology and detection standards aligned with industry standards.

Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for penetration testing of internal corporate network infrastructure and GT production cloud products at least annually. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems.

6. PERSONNEL MANAGEMENT

We staff qualified personnel to develop, maintain, and enhance our security program. We train all employees on security policy, processes, and standards relevant to their role and in accordance with industry practice.

Background checks: Where permitted by applicable law, all new employees undergo a third-party background or reference check. In the United States, employment offers are contingent upon the results of a third-party background check. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

ANNEX III – AUTHORIZED SUB-PROCESSORS

Subprocessor	**Purpose**
Microsoft	M365 and infrastructure
Salesforce	Client/prospect database
Hubspot	Marketing platform
LinkedIn	Recruiting
ClickUp	Task management / change control
NetSuite	Accounting/payment processing
Amazon Web Services	Cloud service provider
Zoom	Marketing webinars
Workato	System integrations
Authorize.net	Payment processing
Docebo	GT-University
Gearset	Salesforce backup
Datadog	Cloud logging & analysis

ANNEX IV – STANDARD CONTRACTUAL CLAUSES (SCCs)

Standard Contractual Clauses approved by the European Commission under Decision 2021/914, Module 2 (Controller to Processor) are incorporated by reference.