GTMIFY LEGAL

Data Processing Agreement (DPA)

Version 1.2 PUBLISHED

Last updated May 7, 2026

Data Processing Agreement

This Data Processing Agreement ("DPA") is entered into by and between **GTMify LLC** ("GTMify") and the customer entity that has executed an agreement for the use of GTMify's services ("Customer"). This DPA is incorporated into and forms an integral part of the main agreement between GTMify and the Customer (the "Agreement").

1. Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

- **"Controller"** means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- **"Data Protection Laws"** means all applicable laws and regulations relating to data protection and privacy, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the UK General Data Protection Regulation ("UK GDPR"), and the California Consumer Privacy Act ("CCPA").
- **"Data Subject"** means the identified or identifiable natural person to whom Personal Data relates.
- **"Personal Data"** means any information relating to a Data Subject that is processed by GTMify on behalf of the Customer as a result of the provision of the Services under the Agreement.
- **"Processing"** means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **"Processor"** means the entity which Processes Personal Data on behalf of the Controller.
- **"Services"** means the go-to-market automation services provided by GTMify to the Customer as described in the Agreement.
- **"Sub-processor"** means any third-party processor engaged by GTMify to Process Personal Data in connection with the Services.

2. Subject Matter and Details of Data Processing

This DPA applies to the Processing of Personal Data by GTMify in the course of providing the Services to the Customer. The details of the data processing are described in **Annex I** to this DPA.

3. Roles and Responsibilities

The parties acknowledge and agree that for the purposes of Data Protection Laws, the Customer is the Controller and GTMify is the Processor of the Personal Data. GTMify shall only Process Personal Data on behalf of and in accordance with the Customer's documented instructions.

4. Processor's Obligations

GTMify, as the Processor, agrees to:

- Process Personal Data only for the purposes of providing the Services and in accordance with the Customer's lawful instructions.
- Ensure that all personnel authorized to Process Personal Data are subject to a duty of confidentiality.
- Implement and maintain appropriate technical and organizational measures to protect the security, confidentiality, and integrity of Personal Data, as further detailed in **Annex II**.
- Provide reasonable assistance to the Customer in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights under Data Protection Laws.
- Notify the Customer without undue delay after becoming aware of a Personal Data breach.
- Make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

5. Sub-processing

The Customer acknowledges and agrees that GTMify may engage Sub-processors to Process Personal Data in connection with the provision of the Services. A list of GTMify's current Sub-processors is attached as **Annex III**. GTMify shall provide the Customer with prior written notice of any intended changes concerning the addition or replacement of Sub-processors, thereby giving the Customer the opportunity to object to such changes.

GTMify shall ensure that any Sub-processor it engages is subject to a written agreement that imposes on the Sub-processor data protection obligations that are no less protective than those imposed on GTMify by this DPA.

6. Security of Processing

GTMify shall implement and maintain the technical and organizational security measures set out in **Annex II** to protect Personal Data against accidental or unlawful destruction, loss, alteration,

unauthorized disclosure, or access. These measures are designed to ensure a level of security appropriate to the risk of the Processing.

7. Data Subject Rights

GTMify shall, to the extent legally permitted, promptly notify the Customer if it receives a request from a Data Subject to exercise their rights under Data Protection Laws. GTMify shall provide the Customer with reasonable cooperation and assistance in relation to any such request.

8. International Data Transfers

To the extent that the Processing of Personal Data by GTMify involves a transfer of Personal Data to a country outside the European Economic Area (EEA), the UK, or Switzerland, GTMify shall ensure that such transfers are made in compliance with the requirements of Data Protection Laws. This may include entering into Standard Contractual Clauses (SCCs) or relying on other legally recognized transfer mechanisms.

9. Data Breach Notification

In the event of a Personal Data breach, GTMify shall notify the Customer without undue delay, and in any case within 48 hours of becoming aware of the breach. The notification shall include, at a minimum:

- A description of the nature of the Personal Data breach, including the categories and approximate number of Data Subjects and Personal Data records concerned.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- A description of the likely consequences of the Personal Data breach.
- A description of the measures taken or proposed to be taken by GTMify to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10. Audit Rights

Upon reasonable request, GTMify shall make available to the Customer information necessary to demonstrate compliance with its obligations under this DPA. GTMify shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, at the Customer's expense.

11. Data Return and Deletion

Upon termination of the Agreement, GTMify shall, at the choice of the Customer, delete or return all Personal Data to the Customer, and delete existing copies unless applicable law requires storage of the Personal Data.

12. Term and Termination

This DPA shall remain in effect for as long as GTMify Processes Personal Data on behalf of the Customer under the Agreement. The provisions of this DPA shall survive the termination of the Agreement for as long as GTMify continues to Process Personal Data.

13. Compliance Certifications and Audits

GTMify is committed to maintaining robust security and compliance standards. While GTMify is working toward obtaining SOC 2 Type II certification, the company implements security controls consistent with SOC 2 Trust Service Criteria, including:

- **Security (CC):** Comprehensive access controls, encryption, monitoring, and incident response procedures.
- **Availability (A):** Redundant infrastructure, automated backups, and disaster recovery capabilities.
- **Processing Integrity (PI):** Data validation, system monitoring, and error handling procedures.
- **Confidentiality (C):** Data classification, access restrictions, and encryption of sensitive information.
- **Privacy (P):** Privacy notice compliance, consent management, and data subject rights fulfillment.

GTMify shall provide the Customer with copies of relevant audit reports, security assessments, and compliance certifications upon request.

14. Data Protection Impact Assessment

GTMify acknowledges that the Customer may be required to conduct a Data Protection Impact Assessment (DPIA) under applicable Data Protection Laws. GTMify shall provide reasonable assistance to the Customer in conducting any such assessment and shall provide information regarding its Processing activities and security measures as necessary.

15. Limitation of Liability

Except as otherwise provided in the Agreement, neither party shall be liable to the other for any indirect, incidental, special, consequential, or punitive damages arising out of or related to this DPA, regardless of the form of action and whether or not such party has been advised of the possibility of such damages.

16. Governing Law and Dispute Resolution

This DPA shall be governed by and construed in accordance with the laws of the jurisdiction specified in the Agreement. Any disputes arising out of or relating to this DPA shall be resolved in accordance with the dispute resolution procedures set forth in the Agreement.

Annex I: Details of Processing

A. List of Parties

- **Data Controller:** The Customer, as defined in the Agreement.
- **Data Processor:** GTMify LLC.

B. Subject Matter, Duration, Nature, and Purpose of the Processing

- **Subject Matter:** The Processing of Personal Data in connection with the provision of GTMify's go-to-market automation services.
- **Duration:** The term of the Agreement.
- **Nature and Purpose:** To enable the Customer to use the Services for automated email and LinkedIn marketing, AI-powered copywriting, lead list generation and enrichment, intent detection, content publishing and engagement, and other related go-to-market activities.

C. Categories of Data Subjects

The Personal Data Processed will concern the following categories of Data Subjects:

- Prospects, customers, and business contacts of the Customer.
- Employees or other representatives of the Customer who use the Services.

D. Categories of Personal Data

The Personal Data Processed will include the following categories of data:

- **Contact Information:** Name, email address, phone number, job title, company name, and social media profiles (e.g., LinkedIn URL).
- **Professional Information:** Employment history, skills, and other information available on public profiles.
- **Technical Information:** IP address, browser type, and other information collected through cookies and similar technologies.
- **Engagement Data:** Information about interactions with marketing campaigns, such as email opens, clicks, and replies.

Annex II: Technical and Organizational Security Measures

GTMify implements the following technical and organizational security measures to protect Personal Data, designed to ensure compliance with SOC 2 Trust Service Criteria and Data Protection Laws:

A. Infrastructure Security

GTMify's services are hosted on PlatformOS, which leverages Amazon Web Services (AWS) infrastructure. This includes:

- **Physical Security:** AWS data centers are secured with physical access controls, surveillance, environmental controls, and other measures to prevent unauthorized access.
- **Network Security:** Use of firewalls, security groups, and network access control lists to restrict access to the network and implement defense-in-depth principles.
- **DDoS Protection:** AWS Shield provides protection against Distributed Denial of Service (DDoS) attacks at the network and application layers.
- **Redundancy and Failover:** Multi-Availability Zone (Multi-AZ) deployment ensures high availability and automatic failover in case of infrastructure failure.

B. Data Encryption

- **Data in Transit:** All data transmitted between the Customer and the Services, and between the Services and Sub-processors, is encrypted using TLS 1.2 or higher (TLS/SSL).
- **Data at Rest:** Personal Data stored within the Services is encrypted at rest using industry-standard encryption algorithms (e.g., AES-256) with encryption keys managed by AWS Key Management Service (KMS).
- **Encryption Key Management:** Encryption keys are securely managed, rotated regularly, and access is restricted to authorized personnel only.

C. Access Control

- **Authentication:** Access to the Services is protected by multi-factor authentication (MFA) where applicable and strong password policies.
- **Authorization:** Role-based access control (RBAC) is used to ensure that users only have access to the information and functionality necessary for their roles.
- **Least Privilege:** The principle of least privilege is applied to both human and programmatic access, with regular reviews of access permissions.
- **Session Management:** Secure session management with automatic timeout and re-authentication for sensitive operations.

D. Vulnerability Management

- **Vulnerability Scanning:** Regular vulnerability scanning of the platform and infrastructure using automated tools and manual assessments.
- **Patch Management:** A process for timely application of security patches and updates to operating systems, applications, and dependencies.
- **Dependency Scanning:** Automated scanning of application dependencies for known vulnerabilities.
- **Remediation:** Critical vulnerabilities are prioritized for immediate remediation.

E. Logging and Monitoring

- **Audit Logs:** Comprehensive logging of access and activity within the Services, including user actions, API calls, and system events.
- **Log Retention:** Logs are retained for a minimum of 90 days and archived for longer-term retention.
- **Monitoring:** Continuous monitoring of the platform for security events and anomalies using automated tools and manual review.
- **Alerting:** Automated alerting for suspicious activities and security events.

F. Incident Response

- **Incident Response Plan:** A documented incident response plan to address security incidents in a timely and effective manner.
- **Incident Classification:** Procedures for classifying incidents by severity and impact.
- **Response Team:** A designated incident response team available 24/7 to respond to security incidents.
- **Breach Notification:** A process for notifying customers of Personal Data breaches in accordance with this DPA and applicable law.
- **Post-Incident Review:** Procedures for conducting post-incident reviews and implementing corrective measures.

G. Personnel Security

- **Confidentiality:** All GTMify employees and contractors are subject to confidentiality obligations and sign confidentiality agreements.
- **Security Training:** Regular security awareness training for all personnel, with emphasis on data protection and privacy.
- **Background Checks:** Appropriate background checks are conducted for personnel with access to sensitive information.
- **Access Termination:** Procedures for promptly terminating access when personnel leave the organization.

H. Business Continuity and Disaster Recovery

- **Backup Procedures:** Regular automated backups of all Personal Data with redundant storage across multiple geographic locations.
- **Disaster Recovery Plan:** A documented disaster recovery plan with defined recovery time objectives (RTO) and recovery point objectives (RPO).
- **Testing:** Regular testing of backup and disaster recovery procedures to ensure effectiveness.
- **Data Restoration:** Procedures for restoring data in the event of data loss or corruption.

I. Vendor Management

- **Vendor Assessment:** Security assessments of all Sub-processors before engagement.
- **Contractual Obligations:** Written agreements with all Sub-processors imposing data protection obligations consistent with this DPA.
- **Ongoing Monitoring:** Periodic review of Sub-processor security practices and compliance.
- **Remediation:** Procedures for addressing non-compliance by Sub-processors.

J. Data Minimization and Retention

- **Minimization:** GTMify processes only the Personal Data necessary to provide the Services.
- **Retention Periods:** Personal Data is retained only for as long as necessary to provide the Services or as required by applicable law.
- **Deletion:** Procedures for secure deletion of Personal Data when it is no longer needed.
- **Anonymization:** Where appropriate, Personal Data is anonymized or pseudonymized to reduce privacy risks.

Annex III: List of Sub-processors

GTMify uses the following Sub-processors to provide the Services. The list is grouped by function for clarity. Locations indicate the primary jurisdiction of the Sub-processor.

Hosting & Infrastructure

Sub-processor	Purpose	Location
PlatformOS	Hosting, authentication, and API management for the GTMify application	United States
Amazon Web Services (AWS)	Underlying cloud infrastructure (via PlatformOS) — compute, storage, KMS	United States

Sub-processor	Purpose	Location
Cloudflare	DNS, CDN, web security, and edge compute (Workers) for microsites and APIs	United States
Vercel	Frontend deployment for microsites and Insights Brief	United States
Railway	Hosting for the Paperclip agent control plane	United States
Supabase	Postgres database, vector storage, edge functions, and file storage	United States
Porkbun	Domain registration	United States
GitHub	Source control and continuous integration / deployment	United States

AI & Large Language Models

Sub-processor	Purpose	Location
Anthropic	Claude family LLMs — reasoning, analysis, and copy generation	United States
OpenAI	Generative AI for onboarding flows and copy generation	United States
OctaveHQ	AI-powered copywriting and prospect-specific message generation	United States
Manus.im	Deep company research, whitepaper generation, and content creation	United States
Google (Gemini)	Account intelligence generation	United States
OpenRouter	Multi-model API gateway providing access to 200+ language models	United States

Workflow & Orchestration

Sub-processor	Purpose	Location
n8n	Visual workflow orchestration for SaaS-to-SaaS automation chains	Germany
Trigger.dev	Durable execution platform for long-running and LLM retry workloads	United States
Paperclip	AI agent control plane — agent org chart and dispatch	United States

Lead Sourcing & Discovery

Sub-processor	Purpose	Location
Apollo.io	Lead and account list generation, ICP search	United States
Vayne	LinkedIn Sales Navigator scraping and enrichment	France
Captain Data	LinkedIn extraction primitives — profile activity, post commenters, post likers	France
Sumble	Lead sourcing and prospecting	United States
Discolike	Lookalike account discovery via natural-language and domain matching	United States (California)
Ocean.io	Lookalike list generation	Denmark
Apify	Web scraping and data collection	Czech Republic

Contact Enrichment & Verification

Sub-processor	Purpose	Location
Brandfetch	Logo, domain, and firmographic enrichment kickoff	Switzerland
Signaliz	GTM enrichment — primary cascade entry	United States
Deepline	Routed second-layer enrichment waterfall	United States
LeadMagic	Email discovery (within Deepline cascade)	United States
Prospeo	B2B lead intelligence and contact enrichment	France
BetterContact	Multi-source contact enrichment	France
People Data Labs	Identity graph and reverse lookup from personal email	United States
BounceBan	Bounce verification and catch-all detection	United Kingdom

Intent & Visitor Identification

Sub-processor	Purpose	Location
RB2B	Onsite intent and visitor deanonymization	United States
Warmly	Onsite intent, visitor auto-trigger, and chat	United States
Delivr.ai	Identity resolution and on-site / off-site signal monitoring	United States

Sub-processor	Purpose	Location
Common Room	Customer intelligence — community, product, and social intent signals	United States
Gojiberry	Competitor engagement signals and survey-driven intent	United States
Kwanzoo	Onsite and offsite intent data	United States

Content & Social Engagement

Sub-processor	Purpose	Location
SuperGrow	LinkedIn content publishing and audience engagement	United States
PitchGhost	Prospect content engagement monitoring	United States

Email Sending & Deliverability

Sub-processor	Purpose	Location
Instantly.ai	Cold email infrastructure and sending	United States
ScaledMail	Email infrastructure and mailbox warming	United States
MailReef	Email infrastructure and deliverability	United States
Masterinbox	Unified inbox across email channels	United States

Multi-Channel Outreach

Sub-processor	Purpose	Location
Lemlist	Multi-channel email and LinkedIn sequences	France
Reply.io	Email and LinkedIn outreach automation; sequence build, sending, reply detection, activity sync	United States
Gojiberry	LinkedIn automation sequences and engagement	United States

CRM & Pipeline

Sub-processor	Purpose	Location
Clarify.ai	Customer relationship management — contacts, companies, pipeline	United States

Channel Delivery

Sub-processor	Purpose	Location
Scribe	Robot-handwritten cards and direct mail (where activated by the Customer)	United States

Meeting & Scheduling

Sub-processor	Purpose	Location
cal.com	Meeting scheduling and call booking	Germany
Reclaim.ai	Calendar coordination and meeting auto-scheduling	United States

Analytics

Sub-processor	Purpose	Location
PostHog	Product analytics and tracking	United States

Operations & Productivity

Disclosed for transparency. These tools support GTMify's internal operations and may incidentally process Personal Data through email, calendar, contracts, and team coordination.

Sub-processor	Purpose	Location
Google Workspace	Email, documents, calendar, and team collaboration	United States
Slack	Real-time team communication and alerts	United States
Stripe	Payment processing and billing	United States
DocuSeal	Contract signing and document workflows	Cyprus
Linear	Engineering task tracking	United States
ClickUp	Operations and client delivery task tracking	United States
Superhuman	Email client	United States
Wispr Flow	Voice-to-text dictation	United States
Mercury	Business banking	United States
QuickBooks Online (Intuit)	Accounting and invoicing	United States

For questions about this DPA or GTMify's data protection practices, please contact hello@gtmify.io.