Data Processing Agreement

Effective 2026-04-27. This Data Processing Agreement ("DPA") forms part of the agreement between Taktly, Inc. ("Taktly", "we", "us", "Processor") and the customer identified in the applicable Order Form or subscription terms ("Customer", "you", "Controller"). It governs Taktly's processing of Personal Data on Customer's behalf in connection with the Taktly platform and services (the "Service").

This DPA is designed to comply with Article 28 of the EU General Data Protection Regulation (GDPR), the UK GDPR, and the California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA). It reflects the technical and organizational measures Taktly has in place to protect Customer Personal Data.

1. Definitions

Capitalized terms not defined here have the meaning given in the underlying agreement or in applicable Data Protection Laws. "Personal Data," "Processing," "Controller," "Processor," "Data Subject," and "Personal Data Breach" carry the meanings given in the GDPR.

"Sub-processor" means any third party engaged by Taktly to Process Customer Personal Data on Taktly's behalf in connection with delivering the Service.

"Customer Personal Data" means Personal Data that Customer or its end users submit to the Service, or that Taktly processes on Customer's behalf in connection with the Service.

2. Subject matter and duration

Taktly processes Customer Personal Data only to provide and improve the Service, and only on documented instructions from Customer. The duration of processing matches the term of the underlying subscription, plus any retention period required by law.

3. Nature and purpose of processing

The Service helps Customer's authorized users plan, run, and document continuous-improvement projects. Personal Data is processed for purposes including: account creation and authentication; project workspace functionality; AI-assisted coaching; PDF artifact generation; subscription billing; product support; and analytics necessary to operate and secure the Service.

4. Types of Personal Data

- Account data: full name, work email, encrypted password hash.
- Profile/branding data: company name, role, optional logo and brand color.
- Project content: any text, file, or data Customer's users enter into the Service (charters, problem statements, root cause analyses, action plans, etc.).
- Usage data: timestamps, IP addresses (hashed), feature events, and audit logs needed for security and operations.
- Billing data: handled by Stripe as an independent processor; Taktly does not store payment card numbers.

5. Categories of data subjects

- Customer's employees, contractors, and authorized end users.
- Where Customer chooses to enter participant or third-party Personal Data into project artifacts (e.g. interviewees in a Voice of the Customer analysis), those individuals are also Data Subjects under this DPA.

6. Customer (Controller) obligations

Customer is the Controller of Customer Personal Data. Customer represents and warrants that:

- It has a lawful basis to provide Customer Personal Data to Taktly for processing.
- It has provided required notices to and obtained any required consents from Data Subjects.
- Its instructions to Taktly comply with applicable Data Protection Laws.

7. Taktly (Processor) obligations

Taktly will:

- Process Customer Personal Data only on Customer's documented instructions, including with regard to international transfers.
- Ensure that personnel authorized to process Customer Personal Data are bound by confidentiality.
- Implement and maintain the technical and organizational measures described in Annex 2.
- Engage Sub-processors only as set out in Section 8 of this DPA.
- Assist Customer, taking the nature of processing into account, with responding to Data Subject requests.
- Notify Customer of Personal Data Breaches affecting Customer Personal Data without undue delay (target: within 72 hours of becoming aware).
- On termination, delete or return Customer Personal Data as set out in Section 13.
- Make available all information necessary to demonstrate compliance with this DPA.

8. Sub-processors

Customer authorizes Taktly to engage Sub-processors. The current list of Sub-processors is published at https://gettaktly.com/trust and includes Supabase (database, auth, storage), Vercel (hosting), Stripe (billing), and Resend (transactional email). Taktly will give Customer at least 30 days' notice before adding a new Sub-processor; Customer may object on reasonable data-protection grounds within that period.

Each Sub-processor is bound by written terms imposing data-protection obligations no less protective than those in this DPA.

9. Data subject rights

Taking into account the nature of the processing, Taktly will provide reasonable assistance to Customer in fulfilling its obligation to respond to Data Subject requests under applicable Data Protection Laws. The Service includes self-service tools for export and deletion that Customer may use to fulfill most requests

directly. For complex requests, contact hello@gettaktly.com.

10. Personal Data Breach notification

Taktly will notify Customer without undue delay (target: within 72 hours of becoming aware) of any confirmed Personal Data Breach affecting Customer Personal Data. The notification will include, to the extent known, the nature of the breach, categories and approximate number of Data Subjects and records affected, likely consequences, and measures taken or proposed to address the breach.

11. Data Protection Impact Assessment (DPIA)

Taktly will provide reasonable assistance to Customer with any DPIA or prior consultation with supervisory authorities required under Article 35 or 36 of the GDPR, taking into account the nature of the processing and the information available to Taktly.

12. Audit

Taktly will make available to Customer information reasonably required to demonstrate compliance with this DPA. Where Customer requires additional audits, the parties will agree on scope, timing, and cost. Taktly may satisfy audit obligations through third-party certifications or attestations (e.g. SOC 2 reports, when available).

13. International transfers

Where Customer Personal Data is transferred outside the EEA, UK, or Switzerland, the parties will rely on Standard Contractual Clauses (SCCs) approved by the European Commission, the UK Addendum where applicable, or another lawful transfer mechanism. The SCCs are deemed incorporated into this DPA by reference where required.

14. Return or deletion of Customer Personal Data

On termination of the Service, Taktly will delete or return all Customer Personal Data within 30 days at Customer's option, except where retention is required by law. Customer may also self-serve deletion at any time using the Reset Workspace feature in Settings or by emailing hello@gettaktly.com with the subject "Delete my account."

15. Liability

Each party's liability under this DPA is subject to the limitations of liability set out in the underlying agreement.

16. Governing law

This DPA is governed by the law specified in the underlying agreement. Where the underlying agreement is silent, the laws of the State of Delaware (USA) apply.

17. Order of precedence

If there is a conflict between this DPA and the underlying agreement, the terms of this DPA prevail with respect to the processing of Customer Personal Data.

18. Contact

- General questions: hello@gettaktly.com
- Security issues and breach notifications: security@gettaktly.com

Annex 1 - Description of processing

Categories of data subjects

- Customer's employees, contractors, and authorized end users.
- Third parties whose Personal Data Customer chooses to enter into project artifacts (e.g. interview subjects, action owners).

Categories of Personal Data

- Identification: name, email address, role.
- Account credentials: bcrypt-hashed password (Taktly never sees plaintext).
- Project content: any free-form text or file Customer enters into the Service.
- Technical: hashed IP address, user-agent string, session identifiers, audit log entries.
- Billing: limited to subscription metadata; full card data handled by Stripe.

Sensitive categories

- Taktly is not designed to process Special Categories of Personal Data (e.g. health data, government identifiers). Customer is responsible for not entering such data into the Service unless a separate written agreement (e.g. HIPAA BAA) is in place.

Frequency of processing

- Continuous, for the duration of the subscription.

Nature of the processing

- Storage; retrieval; display; transmission to authorized users; transmission to Sub-processors as listed at https://gettaktly.com/trust; PDF artifact generation; analytics for service operation and security.

Purpose of the processing

- Provision of the Service; security; product improvement; billing; support; legal compliance.

Duration of processing

- Duration of the subscription, plus retention required by law (typically 7 years for billing records).

Annex 2 - Technical and organizational measures

Taktly maintains the following technical and organizational measures to protect Customer Personal Data. Specific implementations may evolve to reflect industry best practices; protections will not be reduced below the standards described here without notice to Customer.

Encryption

- Encryption in transit using TLS 1.2 or higher for all connections to the Service.
- Encryption at rest using AES-256 for the production database, file storage, and database backups.

Access control

- Authentication via Supabase Auth with bcrypt-hashed passwords; magic-link sign-in option.
- Row-level security (RLS) policies enforced at the database layer for every Customer-tenant table.
- Administrative access restricted to a documented allowlist of email addresses; admin actions are logged.
- Principle of least privilege applied to all internal access to production systems.

Operational security

- Production infrastructure hosted on Supabase (AWS US-East) and Vercel.
- Daily automated backups with point-in-time recovery via Supabase.
- Quarterly testing of backup restoration procedures.
- Vulnerability monitoring through dependency scanning and platform-provided alerts.
- Patch management: critical security patches applied within 7 days of disclosure.

Personnel and process

- Personnel with access to Customer Personal Data are bound by written confidentiality obligations.
- Documented incident response runbook covering detection, containment, notification, and post-incident review.
- Annual review of this Annex and the underlying technical and organizational measures.

Sub-processor management

- Each Sub-processor is bound by written terms requiring at least the same level of data protection as this DPA.
- Customer is notified of new Sub-processors at least 30 days before they begin processing Customer Personal Data.

Annex 3 - List of Sub-processors

The current list of Sub-processors is also maintained at https://gettaktly.com/trust and is updated whenever a Sub-processor is added or removed.

Supabase

Purpose: Postgres database, authentication, file storage
Region: AWS US-East
Compliance: SOC 2 Type II, HIPAA-eligible

Vercel

Purpose: Application hosting, edge network, TLS termination
Region: Global edge, US-East primary
Compliance: SOC 2 Type II, ISO 27001

Stripe

Purpose: Subscription billing and payment processing
Region: United States
Compliance: PCI-DSS Level 1, SOC 1, SOC 2 Type II

Resend

Purpose: Transactional email delivery
Region: United States
Compliance: SOC 2 Type II

Acceptance

By executing the underlying subscription agreement or Order Form, or by clicking to accept Taktly's Terms of Service, Customer accepts this Data Processing Agreement. Customers requiring a counter-signed copy may sign below and return to hello@gettaktly.com.

Customer (Controller)

Company name: _____

Authorized signatory: _____

Title: _____

Email: _____

Date: _____

Signature: _____

Taktly (Processor)

Company: Taktly, Inc.
Authorized signatory: Vernon Lee
Title: Founder & CEO
Email: hello@gettaktly.com
Date: 2026-04-27

Signature: _____