Data Processing Agreement (DPA) V1.3

This Data Processing Agreement (“Agreement”) is issued by **TimelinesAI LLC** (“Processor”) and forms part of the **Terms of Service** or any other applicable agreement governing the use of TimelinesAI services (the “Principal Agreement”).

By subscribing to, accessing, or using TimelinesAI services, the customer (“Controller”) is deemed to have accepted and agreed to this Agreement.

This Agreement is not open to negotiation and applies automatically to all customers to the extent required by Article 28 of the GDPR.

1. Definitions

"GDPR" refers to the General Data Protection Regulation (EU) 2016/679.

"Personal Data" means any information relating to an identified or identifiable natural person. "Processing" means any operation performed on Personal Data, such as collection, storage, or transmission.

"Sub-Processor" means any third-party entity engaged by the Processor to process Personal Data on behalf of the Controller.

2. Subject Matter & Purpose

The Controller has engaged the Processor to provide SaaS services that involve the processing of Personal Data.

The Processor shall process Personal Data only for the purposes specified by the Controller, in accordance with this Agreement, and shall not process Personal Data for its own purposes.

3. Obligations of the Processor

The Processor shall:

- Process Personal Data only in accordance with the documented instructions of the Controller;
- Ensure that personnel authorized to process Personal Data are subject to confidentiality obligations;
- Implement appropriate **technical and organizational measures (TOMs)** to ensure data security (see Annex II);
- Assist the Controller in fulfilling its obligations regarding Data Subject rights and cooperation with supervisory authorities;
- Assist the Controller, upon request, in fulfilling its obligations under Articles 32–36 GDPR, including Data Protection Impact Assessments;
- Notify the Controller without undue delay in the event of a data breach;

4. Obligations of the Controller

The Controller shall:

- Ensure that Personal Data is lawfully collected and provided to the Processor;
- Provide clear and documented instructions to the Processor regarding data processing;

- Inform the Processor of any changes in processing requirements or legal obligations.

5. Security Measures

The Processor shall implement the Technical and Organizational Measures (TOMs) described in **Annex II**. These include, but are not limited to: encryption, access control, authentication, backups, monitoring, and regular security audits.

6. Sub-Processors

- The Controller grants general authorization for the Processor to engage Sub-Processors listed in **Annex I**.
- The Processor shall ensure that each Sub-Processor is bound by equivalent data protection obligations.
- The Processor may update the list of subprocessors from time to time and will make information about such changes available to the Controller upon request.

7. International Data Transfers

If Personal Data is transferred outside the EEA, the Processor shall ensure appropriate safeguards such as:

- Standard Contractual Clauses (SCCs);
- Binding Corporate Rules (BCRs);
- Other approved mechanisms under GDPR.

8. Data Breach Notification

The Processor shall notify the Controller without undue delay, and no later than 48 hours, after becoming aware of a data breach. The notification shall include details of the breach, its likely impact, and remediation measures.

9. Audit and Compliance

Upon written request, the Processor shall provide evidence of its data protection and security practices (e.g., security certifications, audit summaries, or responses to a questionnaire). No on-site audits shall be permitted unless required by law.

10. Term & Termination

This Agreement shall remain in effect as long as the Processor processes Personal Data on behalf of the

Controller.
Upon termination, the Processor shall delete or return all Personal Data within **30 days**, unless retention is required by applicable law.

11. Liability & Indemnification

Each party shall be liable for any breaches of this Agreement in accordance with applicable data protection laws.
The Processor shall not be liable for indirect or consequential damages resulting from compliance with the Controller’s instructions.

12. Governing Law & Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of the State of Wyoming, USA, without regard to its conflict of law principles.

Any disputes arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the state and federal courts located in Wyoming, USA.

13. Acceptance

This Agreement is deemed executed and binding on both parties when the Controller subscribes to or uses TimelinesAI services.

No physical signature is required for its validity or enforceability.

Annex I – List of Subprocessors

TimelinesAI engages the following subprocessors:

- **Amazon Web Services (AWS)** – Cloud hosting (EU region)
- **Google Cloud Platform** – Cloud hosting (EU region)
- **Azure** - Cloud hosting (EU region)
- **Intercom** – Customer support messaging
- **PostHog** – Application analytics (EU region)
- **Stripe** - Payment processor

Annex II – Technical and Organizational Measures (TOMs)

TimelinesAI implements the following TOMs to protect Personal Data:

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256);
- Role-based access control and multi-factor authentication for the internal services;
- Daily encrypted backups stored securely;
- Incident response procedures and breach reporting within 48 hours;
- Employee confidentiality agreements and annual security training;
- Secure software development lifecycle (SDLC) and code review practices;
- Periodic review and update of security measures.

Annex III – Categories of Data Subjects and Personal Data

Categories of Data Subjects:

Users authorized by the Controller to access the service; individuals whose personal data appears in the Controller's communications managed within the TimelinesAI platform.

Categories of Personal Data:

Contact details, communication content and metadata, and usage data required for service operation and analytics.

End of Agreement