

AppoByte Data Processing Addendum (DPA)

Last Updated: 1/16/2026

This Data Processing Addendum ("DPA") forms part of the agreement between **AppoByte, Inc.** ("AppoByte," "we," "us") and the customer entity that has entered into the AppoByte Master Terms of Service or other applicable agreement referencing this DPA ("Customer," "you"). This DPA applies to the extent AppoByte processes Personal Data on behalf of Customer in the course of providing the Services.

In the event of a conflict between this DPA and the Master Terms of Service, this DPA controls solely with respect to data protection and privacy matters.

1. Definitions

- **"Applicable Data Protection Laws"** means all laws and regulations applicable to the processing of Personal Data, including U.S. federal and state privacy laws.
- **"Personal Data"** means any information relating to an identified or identifiable individual processed by AppoByte on behalf of Customer.
- **"Processing"** has the meaning given under Applicable Data Protection Laws.
- **"Sub-Processor"** means a third party engaged by AppoByte to process Personal Data.

2. Roles of the Parties

Customer is the controller of Personal Data, and AppoByte is the processor, except where AppoByte acts as a controller under its Privacy Policy.

Customer represents that it has all necessary rights and lawful bases to provide Personal Data to AppoByte for processing.

3. Scope and Purpose of Processing

AppoByte will process Personal Data solely to:

- Provide, operate, and support the Services
- Maintain the security and integrity of the Services
- Comply with applicable legal obligations

Processing may occur across multiple AppoByte-owned applications, platforms, or AI agents, solely for the purposes described above.

4. Customer Instructions

Customer instructs AppoByte to process Personal Data in accordance with:

- This DPA
- The applicable Order Form
- Customer's documented, lawful instructions

AppoByte will notify Customer if it believes an instruction violates Applicable Data Protection Laws.

5. Confidentiality

AppoByte will ensure that personnel authorized to process Personal Data are bound by confidentiality obligations no less protective than those set forth in this DPA.

6. Security Measures

AppoByte will implement and maintain commercially reasonable administrative, technical, and organizational safeguards designed to protect Personal Data against unauthorized access, disclosure, alteration, or destruction.

High-level descriptions of security measures are set forth in Annex B.

7. Sub-Processors

Customer authorizes AppoByte to engage Sub-Processors to process Personal Data. AppoByte will:

- Maintain a list of Sub-Processors available upon request or via a designated URL
- Impose data protection obligations on Sub-Processors consistent with this DPA
- Remain responsible for Sub-Processors' compliance with this DPA

AppoByte will provide reasonable advance notice of material changes to Sub-Processors and allow Customer to object on reasonable grounds.

8. Data Subject Rights Assistance

To the extent required by Applicable Data Protection Laws, AppoByte will provide reasonable assistance to Customer in responding to requests from data subjects to exercise their rights, taking into account the nature of the processing.

9. Incident and Breach Notification

AppoByte will notify Customer **without undue delay after becoming aware of a confirmed Personal Data breach**, and will provide available information necessary to support Customer's compliance with applicable data protection laws.

10. Data Retention, Return, and Deletion

Upon termination of the Services, AppoByte will, at Customer's request and subject to applicable law:

- Return Personal Data to Customer, or
- Delete Personal Data

AppoByte may retain Personal Data where required by law or for legitimate business purposes consistent with this DPA.

11. Audits and Compliance

Upon reasonable written request, AppoByte will provide information reasonably necessary to demonstrate compliance with this DPA. Formal audits are limited to one per year and subject to confidentiality and security restrictions.

12. Artificial Intelligence and Automated Processing

Certain Services may include artificial intelligence or automated processing features. Unless expressly agreed in writing:

- Customer Personal Data is not used to train shared or general-purpose AI models
- AI Outputs may be probabilistic and require independent validation by Customer
- AppoByte does not guarantee the accuracy of AI-generated outputs

13. Liability and Precedence

Liability arising from this DPA is subject to the limitations set forth in the Master Terms of Service.

14. Governing Law

This DPA is governed by the laws of the State of Florida, without regard to conflict of law principles.

Annex A – Processing Details

- **Categories of Data Subjects:** End users, employees, contractors, customers
- **Categories of Personal Data:** Contact information, usage data, content submitted to the Services
- **Processing Activities:** Hosting, storage, transmission, analysis, support
- **Duration of Processing:** For the duration of the applicable Subscription Term

Annex B – Security Measures

AppoByte maintains administrative, technical, and organizational safeguards designed to protect Personal Data, including but not limited to:

- Role-based access controls and authentication mechanisms
- Encryption of data in transit using TLS 1.2 or higher
- Encryption of stored data where supported by the infrastructure provider
- Security monitoring, logging, and incident detection mechanisms
- Incident response procedures for security events
- Periodic security reviews and vulnerability management practices

Additional details regarding AppoByte's security practices and infrastructure safeguards are available through the [AppoByte Trust Center](#).

Contact for Data Protection Matters

AppoByte, Inc. | Tampa, Florida | apps@appobyte.com