

Data Processing Addendum (DPA)

Last Updated: January 1, 2026

This Data Processing Addendum (“**DPA**”) forms part of the Terms of Service between **PYBK, Inc.**, doing business as **Playbook** (“**Playbook**” or “**Processor**”), and the customer entity (“**Customer**” or “**Controller**”), to the extent Playbook processes Personal Data on Customer’s behalf in connection with the Services.

Capitalized terms not defined in this DPA have the meanings set forth in the Terms of Service.

1. Scope and Applicability

1.1 Roles

- Customer is the **Controller** of Personal Data contained in Customer Content.
- Playbook acts as a **Processor** of such Personal Data when processing it on Customer’s behalf.

1.2 Applicable Laws

This DPA applies to Personal Data subject to applicable data protection laws, including the **GDPR**, **UK GDPR**, and other comparable global privacy and data protection laws.

2. Details of Processing

2.1 Subject Matter

Processing of Customer Content and related Personal Data to provide, operate, secure, support, and improve the Services.

2.2 Duration

For the term of the applicable subscription and any post-termination retention period described in the Privacy Policy.

2.3 Categories of Data Subjects

Customer’s users, employees, contractors, vendors, guest users, and other individuals whose data is submitted to the Services.

2.4 Types of Personal Data

Contact information, identifiers, usage data, communications, documents, metadata, and other data uploaded or generated through use of the Services.

2.5 Processing Activities

Hosting, storage, transmission, retrieval, analysis, backup, monitoring, troubleshooting, support, and AI-assisted processing.

3. Processor Obligations

Playbook shall:

- Process Personal Data only on documented instructions from Customer, including as set forth in the Terms of Service
- Ensure personnel are subject to confidentiality obligations
- Implement appropriate technical and organizational measures to protect Personal Data
- Not sell Personal Data
- Not process Personal Data in a manner that allows identification or reconstruction of individual customers or disclosure of one customer's data to another

Nothing in this DPA restricts Playbook's ability to use **aggregated, anonymized, de-identified, or derived data** (including metadata, embeddings, usage patterns, and system outputs) for purposes of operating, improving, securing, and developing the Services, provided such data does not identify Customer or individuals.

4. Customer Obligations

Customer represents and warrants that:

- It has all rights, permissions, and lawful bases to provide Personal Data to Playbook
- It has provided required notices and obtained required consents
- Its instructions comply with applicable law

Customer is solely responsible for the accuracy, quality, and legality of Personal Data.

5. Subprocessors

5.1 General Authorization

Customer grants Playbook general authorization to engage subprocessors to process Personal Data.

5.2 Subprocessor Obligations

Playbook shall impose data protection obligations on subprocessors that are no less protective than those in this DPA.

5.3 Changes and Notice

Playbook may update its subprocessors from time to time and will provide reasonable notice of material changes. Customer may object to a new subprocessor on reasonable data protection grounds.

5.4 Subprocessor List

A current list of subprocessors may be made available on Playbook's website or upon request.

6. Security Measures

Playbook implements **commercially reasonable technical and organizational measures** designed to protect Personal Data against unauthorized access, loss, alteration, or disclosure, consistent with industry standards.

Playbook does not guarantee absolute security.

7. Personal Data Breach

Playbook shall notify Customer **without undue delay** after becoming aware of a confirmed Personal Data breach, to the extent required by applicable law, and shall provide reasonable cooperation.

8. Data Subject Rights and Regulatory Assistance

Taking into account the nature of the processing, Playbook shall provide **commercially reasonable assistance** to Customer in responding to data subject requests, data protection impact assessments, and regulatory inquiries, to the extent required by applicable law.

9. Data Retention and Deletion

Upon termination of the Services, Personal Data will be retained and deleted in accordance with the Privacy Policy, unless retention is required by law.

10. Audits

Customer may audit Playbook's compliance **only where required by applicable law**, subject to reasonable scope, confidentiality, and frequency limitations. Third-party certifications, attestations, or audit reports may be used to satisfy audit requests.

11. International Data Transfers

11.1 EEA Transfers

Where Personal Data is transferred outside the EEA, the **EU Standard Contractual Clauses (Module 2 – Controller to Processor)** are incorporated by reference.

11.2 UK Transfers

For UK Personal Data, the **UK International Data Transfer Addendum** applies.

11.3 Safeguards

Playbook applies appropriate safeguards and supplementary measures consistent with applicable law.

12. Liability

Liability under this DPA is subject to the limitations of liability set forth in the Terms of Service.

13. Order of Precedence

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

14. Changes

Playbook may update this DPA as required to comply with changes in law. Material changes will be posted on the website.

15. Governing Law

This DPA is governed by the same law and venue as the Terms of Service.

16. Binding Effect

This DPA becomes legally binding upon **Customer's acceptance of the Terms of Service** or **execution of an Order Form or agreement referencing this DPA**, whichever occurs first.