

## Privacy Policy

**Last Updated: January 1, 2026**

**PYBK, Inc.**, doing business as **Playbook** (“**Playbook**,” “**we**,” “**us**,” or “**our**”), provides subscription-based software-as-a-service products, including scheduling, work management, collaboration, document sharing, chat, mobile access, artificial intelligence features, APIs, and related services (collectively, the “**Services**”).

This Privacy Policy explains how we collect, use, disclose, retain, and safeguard **Personal Data** and **Customer Content** in connection with the Services.

By accessing or using the Services, you agree to this Privacy Policy.

### 1. Roles and Scope

For purposes of applicable data protection laws:

- **Playbook acts as a data processor** with respect to Customer Content.
- **Customers act as data controllers** with respect to Customer Content.
- **Playbook acts as a data controller** with respect to account, usage, technical, and marketing data.

This Policy applies to all users of the Services, including administrators, members, guest users, mobile users, and API users.

Customers are solely responsible for configuring user permissions, guest access, API access, and data-sharing settings. Playbook is not responsible for unauthorized access or disclosure resulting from customer-configured permissions or credential sharing.

### 2. Information We Collect

#### A. Account and User Information

- Name, email address, phone number
- Job title and company name
- Authentication and account credentials
- Communications with support or sales

## **B. Usage and Technical Information**

- IP address, device identifiers, browser type
- Logs, timestamps, feature usage
- Cookies and similar technologies

## **C. Customer Content**

Data uploaded, submitted, stored, generated, or processed through the Services, including:

- Documents, files, images, and media
- Chat messages and collaboration records
- Schedules, tasks, work items, and metadata
- Vendor, subcontractor, and contact information

Customer Content remains the property of the customer. Playbook does not claim ownership.

## **3. How We Use Information**

We use information only as necessary to:

- Provide, operate, secure, and support the Services
- Authenticate users and enforce subscription and usage limits
- Enable collaboration, guest access, mobile access, and APIs
- Monitor performance, reliability, and security
- Improve functionality, usability, and AI-powered features
- Generate aggregated, anonymized, or de-identified analytics
- Comply with legal and regulatory obligations

## 4. Artificial Intelligence and Data Analytics

The Services include AI-powered features that may analyze Customer Content, communications, schedules, documents, metadata, and user interactions to provide functionality within the Services.

Playbook's approach to AI and analytics is guided by the following principles:

- **Purpose limitation:** Data is analyzed only to operate, secure, improve, and optimize the Services.
- **Customer isolation:** Customer Content is not analyzed in a manner that allows one customer to access or infer another customer's data.
- **Aggregation, de-identification, and derived data:** Playbook may use aggregated, anonymized, de-identified, or derived data (such as metadata, embeddings, usage patterns, workflow structures, and system outputs) to improve AI systems, features, and overall service performance.
- **No customer data exposure:** Customer Content is not used to train or operate AI models in a manner that allows identification or reconstruction of any individual, customer, project, or workspace.

AI-generated outputs are probabilistic, provided “**as is**,” and may be inaccurate or incomplete. Customers are solely responsible for reviewing and validating outputs prior to reliance.

Additional information regarding AI functionality, limitations, and data usage is described in the **Playbook AI Use Policy** available on our website.

## 5. Legal Bases for Processing (GDPR and Similar Laws)

Where applicable, Playbook processes Personal Data based on:

- Performance of a contract
- Legitimate business interests
- Legal obligations
- Consent, where required

## 6. Data Sharing and Disclosure

We may disclose information only:

- At the customer's direction or with consent
- To service providers acting under confidentiality and security obligations
- To comply with applicable law, regulation, subpoena, or lawful government request
- To protect the rights, security, and integrity of Playbook, users, or the Services
- In connection with a financing, merger, acquisition, reorganization, or sale of assets

Playbook does not sell Personal Data.

## **7. Third-Party Services and APIs**

The Services may integrate with third-party platforms or provide APIs allowing access to data at the customer's direction.

Playbook does not control third-party services and is not responsible for their privacy, security, or data practices. Customers are responsible for authorizing access and ensuring third-party compliance with applicable laws.

## **8. Security**

Playbook maintains commercially reasonable administrative, technical, and organizational safeguards designed to protect information, including encryption in transit, access controls, monitoring, and periodic security reviews.

No system is completely secure. Use of the Services is at your own risk.

## **9. Security Incidents**

In the event of a confirmed security incident affecting Personal Data or Customer Content, Playbook will take reasonable steps to investigate, mitigate, and remediate the incident. Where required by applicable law, Playbook will provide notice to affected customers or individuals.

## **10. Data Retention and Deletion**

- Personal Data is retained only as long as necessary for legitimate business and legal purposes.
- Customer Content is retained for the duration of the subscription and a limited post-termination period to permit data export.
- After expiration, data is deleted or anonymized unless legally required otherwise.

Customers are responsible for exporting data prior to deletion.

## **11. Aggregated and De-Identified Data**

Playbook may create and use aggregated, anonymized, de-identified, or derived data for analytics, benchmarking, product improvement, and business purposes. Such data does not identify any individual or customer.

## **12. Your Rights**

Depending on jurisdiction, individuals may have rights to access, correct, delete, or restrict processing of Personal Data, and to request data portability. Requests are subject to verification and legal limitations.

## **13. International Data Transfers**

The Services are offered globally. Information may be processed in jurisdictions outside your country of residence. Where required, Playbook applies appropriate safeguards consistent with applicable law.

## **14. Children's Privacy**

The Services are not intended for individuals under 18. We do not knowingly collect Personal Data from children.

## **15. Changes to This Policy**

We may update this Privacy Policy from time to time. Continued use of the Services after updates constitutes acceptance of the revised Policy.

## **16. Contact Information**

### **PYBK, Inc.**

Attn: Privacy Officer

Email: **contact@pybk.ai**