# PRIVACY POLICY

Last Updated: Sep 2, 2026

PaleBlueDot AI Inc. and its affiliates (collectively, "PaleBlueDot AI," "PBD," "we," "our," or "us") are committed to protecting personal data and handling it responsibly. This Privacy Policy explains how we collect, use, disclose, store, and otherwise process personal data when you visit our website at www.palebluedot.ai and any associated websites or webpages that link to this Privacy Policy (collectively, the "Website"), create or use a PBD account, or otherwise use our products and services (collectively, the "Services").

This Privacy Policy also describes your choices and rights regarding your personal data. Please read it carefully.

This Privacy Policy does not apply to third-party websites, applications, services, or platforms that we do not control. Those third parties are subject to their own privacy notices, terms, and data handling practices.

If you are an enterprise customer or are using the Services on behalf of an organization, a separate customer agreement, order form, data processing addendum, or other written agreement with us may apply. In the event of a conflict between this Privacy Policy and such written agreement, the written agreement will control to the extent of the conflict.

1. Scope and Roles

Depending on the context in which you use the Services, PBD may act as a data controller, business, processor, or service provider.

When PBD acts as a controller or business, we decide how and why personal data is processed for our own purposes, such as account administration, billing, security, legal compliance, fraud prevention, sales, marketing, and operation of the Website.

When PBD provides Services to an enterprise customer and processes personal data on that customer's behalf, including where a customer submits or routes personal data through the Platform for its own business purposes, PBD may act as a processor or service provider. In those circumstances, the relevant customer is generally responsible for providing any required notices to end users and for obtaining any required consents or other lawful bases for processing.

## 2. Personal Data We Collect

We may collect the following categories of personal data, depending on how you interact with us and the Services:

### 2.1 Account and Contact Information

This may include your name, company name, job title, email address, telephone number, mailing or billing address, account credentials, username, account identifiers, and communication preferences.

### 2.2 Commercial and Billing Information

This may include payment-related information, or prepaid balance history, invoices, transaction records, tax identifiers, billing contacts, payment verification information, and records relating to purchases or subscriptions. Payment card information may be collected and processed directly by our payment processors rather than by PBD.

### 2.3 Compliance and Verification Information

This may include know-your-customer, sanctions screening, export control, anti-money laundering, business verification, beneficial ownership, use case, identity verification, or other compliance-related information that you provide to us or that we obtain from service providers or public sources.

### 2.4 Technical, Device, and Usage Information

This may include IP address, approximate location inferred from IP address, browser type, operating system, device identifiers, user agent, referral URLs, pages viewed, clicks, dates and times of access, authentication events, request volume, latency, error logs, network metadata, and other information about how you access or use the Website or Services.

### 2.5 Support and Communications Information

This may include the contents of your communications with us, such as emails, tickets, chat messages, call notes, meeting notes, feedback, survey responses, and records relating to support, onboarding, or commercial discussions.

### 2.6 Cookies and Similar Technologies Data

When you visit the Website, we and our service providers may use cookies, pixels, SDKs, local storage, and similar technologies to collect data about your device and interactions with the Website. For more information, see Section 11 below.

### 2.7 Information from Third Parties

We may receive personal data from your employer or organization, our affiliates, payment processors, identity verification providers, sanctions screening providers, analytics providers, advertising or marketing partners, social media platforms, resellers,integration partners, and publicly available sources, where permitted by applicable law.

## 3. How We Collect Personal Data

We collect personal data in the following ways:

- Directly from you, such as when you create an account, contact us, purchase Services, submit a support request, sign up for emails, complete forms, or otherwise communicate with us.
- Automatically, such as through server logs, cookies, pixels, SDKs, and other technologies when you visit the Website or use the Services.
- From your organization or account administrators, such as where your employer purchases or administers access to the Services for you.
- From third parties, such as service providers, payment processors, compliance vendors, and publicly available sources.

## 4. How We Use Personal Data

We may use personal data for the following purposes:

- To provide, operate, maintain, secure, and improve the Website and Services.
- To create, administer, authenticate, and manage accounts, credentials, and subscriptions.
- To process transactions, provide billing and invoicing, and administer prepaid balances, top-ups, and service usage.
- To communicate with you about your account, the Services, support matters, incidents, updates, and administrative or operational notices.

- To provide customer service, onboarding, implementation, troubleshooting, and technical support.
- To analyze performance, usage trends, product quality, reliability, fraud patterns, and abuse signals, and to improve functionality and user experience.
- To protect the Website, Platform, Services, users, and third parties from fraud, abuse, misuse, unauthorized access, security incidents, or other harmful activity.
- To conduct compliance checks, sanctions screening, export control reviews, anti-money laundering reviews, and other legal or regulatory diligence.
- To enforce our Terms of Use, customer agreements, Platform Policies, and other legal rights.
- To send marketing or promotional communications, where permitted by law and subject to your choices.
- To comply with applicable laws, regulations, legal process, governmental requests, industry standards, and internal governance requirements.
- To support corporate transactions, financing, audits, insurance, or strategic transactions involving our business.

## 5. How We Disclose Personal Data

We may disclose personal data to the following categories of recipients, subject to applicable law and contractual restrictions:

### 5.1 Affiliates

We may disclose personal data to our affiliates for the purposes described in this Privacy Policy, including account administration, billing, support, legal compliance, security, and business operations.

### 5.2 Service Providers and Contractors

We may disclose personal data to vendors, contractors, consultants, and other service providers that perform services on our behalf, such as cloud hosting, infrastructure, analytics, security, payment processing, communications, customer relationship management, customer support, legal compliance, sanctions screening, and professional advisory services.

### 5.3 Infrastructure Providers

We may disclose Customer Content, technical metadata, and related personal data to cloud providers, and infrastructure providers as necessary to provide the Services,including to process requests, return outputs, and maintain service continuity.

### 5.4 Enterprise Customers and Account Administrators

If you use the Services through an enterprise account, reseller, managed account, or organizational subscription, we may disclose personal data to the relevant customer, reseller, or administrator for account management, billing, usage reporting, support, compliance, and security purposes.

Depending on the product configuration and customer agreement, administrators for your organization may also be able to access or control certain account information, usage information, audit or security logs, billing records, workspace settings, support records, or Customer Content associated with your organizational account.

### 5.5 Payment Processors and Financial Institutions

We may disclose personal data to payment processors, banks, card networks, billing providers, and fraud prevention providers as necessary to process payments, verify transactions, prevent chargebacks, and administer billing.

### 5.6 Legal, Compliance, and Safety Disclosures

We may disclose personal data where we believe in good faith that disclosure is necessary to: (a) comply with applicable law, regulation, legal process, or governmental request; (b) enforce our legal rights, agreements, or policies; (c) protect the rights, safety, security, or property of PBD, our users, customers, providers, or third parties; (d) detect or prevent fraud, abuse, security incidents, or unlawful conduct; or (e) respond to an emergency involving risk of death or serious physical harm.

### 5.7 Corporate Transactions

We may disclose personal data in connection with an actual or proposed financing, audit, merger, acquisition, reorganization, bankruptcy, receivership, sale of assets, or similar corporate transaction, subject to customary confidentiality protections.

### 5.8 At Your Direction or With Your Consent

We may disclose personal data to other parties at your direction or with your consent.

We do not sell personal data for money. We do not share personal data for cross-context behavioral advertising in the manner commonly described under certain U.S. state privacy laws.

## 6. Legal Bases for Processing

If you are located in the European Economic Area, United Kingdom, or Switzerland, we generally rely on one or more of the following legal bases for processing personal data, depending on the circumstances:

- Performance of a contract with you or your organization.
- Compliance with a legal obligation.
- Our legitimate interests, such as operating and improving the Services, securing our systems, preventing fraud, conducting business operations, and marketing our Services to business contacts, provided those interests are not overridden by your fundamental rights and freedoms.
- Your consent, where required by law.

## 7. International Data Transfers

We and our service providers may process personal data in the United States, Singapore, Japan, the European Union, and other jurisdictions in which we or our providers operate. These jurisdictions may have data protection laws that differ from those in yourjurisdiction.

Where required by applicable law, we will use appropriate safeguards for cross-border transfers of personal data, which may include contractual clauses, risk assessments, transfer impact measures, or other lawful transfer mechanisms.

Certain enterprise features may support specific routing, region, residency, or deployment options. If you require specific data location, transfer, or residency commitments, please ensure that such commitments are expressly stated in your written agreement with PBD.

## 8. Data Retention

We retain personal data for as long as reasonably necessary for the purposes described in this Privacy Policy, including to provide the Services, maintain accounts, comply with legal obligations, resolve disputes, enforce agreements, detect and prevent fraud, and protect our rights and interests.

Retention periods vary depending on the type of data, the Services involved, the context in which the data was collected, and our legal or contractual obligations. For example:

- account, billing, and transaction records may be retained for the duration of the relationship and for an additional period needed for accounting, tax, audit, and legal compliance;
- support records may be retained for the period needed to address the issue and maintain a support history;
- optional logs or debugging records may be retained for the duration reasonably necessary to troubleshoot and resolve the relevant issue;
- security, fraud, and compliance records may be retained for the duration needed to investigate, prevent, document, or respond to incidents or legal obligations; and

When we no longer need personal data, we will delete, anonymize, or de-identify it, unless retention is required or permitted by applicable law.

## 9. Security

We use commercially reasonable administrative, technical, and organizational safeguards designed to protect personal data against unauthorized access, loss, misuse, alteration, and disclosure. These safeguards may include encryption in transit using TLS 1.2 or higher, access controls, audit logging, network security controls, vendor diligence, incident response procedures, and role-based access restrictions.

No method of transmission over the internet or method of electronic storage is completely secure. As a result, we cannot guarantee absolute security. You are responsible for maintaining the confidentiality of your credentials and for using appropriate security measures when using the Services.

## 10. Cookies and Similar Technologies

We and our service providers may use cookies, pixels, SDKs, local storage, and similar technologies on the Website for the following purposes:

- to operate, secure, and maintain the Website;
- to remember preferences and settings;
- to understand traffic and usage patterns;
- to diagnose performance issues and improve the Website; and
- where permitted, to support communications, measurement, and marketing activities.

You can control cookies through your browser settings and, where applicable, through cookie banners or consent tools on the Website. If you disable cookies, some parts of the Website may not function properly.

11. Your Rights and Choices

Depending on your location and the circumstances, you may have the right to:

- know whether we process your personal data;
- access or obtain a copy of certain personal data;
- correct inaccurate personal data;
- delete personal data;
- restrict or object to certain processing;
- withdraw consent where processing is based on consent;
- request portability of certain personal data;
- opt out of certain direct marketing communications; and
- appeal our decision where we decline to take action on a request, if such appeal right is available under applicable law.

You may also have the right to object to or opt out of certain profiling or processing for targeted advertising. As stated above, PBD does not sell personal data for money or share personal data for cross-context behavioral advertising as commonly defined under certain U.S. state privacy laws.

To exercise your rights, please contact us by clicking "Contact Us" at the top-left of our homep age. We may need to verifyyour identity or authority before processing your request. We may d eny or limit a request wherepermitted by law.

If you use the Services through an enterprise customer or other organization, you may wish to contact that organization first, because it may control certain processing of your personal data.

12. U.S. State Privacy Disclosures

For residents of California and certain other U.S. states with applicable privacy laws, this section provides additional disclosures.

During the preceding 12 months, we may have collected the following categories of personal data, depending on your use of the Services:

- identifiers and contact information;
- commercial information and transaction data;
- internet or network activity information;
- approximate geolocation derived from IP address;
- professional or employment-related information;
- compliance and verification information;
- support and communications records; and
- Customer Content, where submitted to us, including for support or optional logging.

We may disclose these categories of personal data to affiliates, service providers, enterprise customers or account administrators, payment processors, advisors, authorities, and transaction counterparties for the purposes described in this Privacy Policy.

We do not knowingly sell personal data for monetary consideration. We do not knowingly share personal data for cross-context behavioral advertising. We do not knowingly process sensitive personal data for the purpose of inferring characteristics about individuals, except as permitted by applicable law and as reasonably necessary to provide the Services, comply with law, or protect security.

We do not use personal data to make decisions that produce legal or similarly significant effects on individuals in a manner that would trigger opt-out rights under applicable state privacy law, except as may be necessary for fraud prevention, security, export control, sanctions screening, or legal compliance.

## 13. Children

The Website and Services are not intended for children under 18 years of age, and we do not knowingly collect personal data directly from children under 18. If you believe that a child has provided personal data to us in violation of this Privacy Policy, please contact us and we will take appropriate steps.

## 14. Third-Party Services

The Website and Services may contain links to or integrations with third-party services. This Privacy Policy does not apply to third-party services, and we are not responsible for their privacy practices. We encourage you to review the privacy notices of those third parties.

## 15. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. If we make changes, we will post the revised Privacy Policy on the Website and update the "Last Updated" date above. Where required by law, we will also provide additional notice or obtain consent.

## 16. Contact Us

If you have questions about this Privacy Policy or our privacy practices, or if you would like to exercise your rights, please click "Contact Us" at the top-left of our homepage to reach us.

If you are located in a jurisdiction that permits you to lodge a complaint with a supervisory authority or regulator, you may also have the right to do so.