

PARTA.IO

PRIVACY POLICY

Last Updated: July 30, 2026

This Privacy Policy (the "**Policy**") describes how Parta IO Corp., a Delaware corporation with its principal address at 16192 Coastal Highway, Lewes, Delaware 19958, USA ("**Parta.io**", "**we**", "**us**" or "**our**"), collects, uses, shares and protects personal information in connection with our websites, our online content authoring and orchestration platform, our mobile applications, and the emails we send (collectively, the "**Services**").

This Policy applies to the personal information of visitors to our websites and of the users of the Services (the "**User(s)**", "**you**" or "**your**"), and describes your choices regarding the use, access and correction of your personal information. Capitalized terms used but not defined in this Policy have the meanings given to them in Parta.io's Terms of Service or Master Services Agreement, as applicable (the "**Terms**").

Our Role: Controller and Processor

We process personal information in two distinct capacities:

- Parta.io as controller. We act as a "controller" (or equivalent term under applicable law) of the personal information described in this Policy — including account and registration information, billing and business contact information, information collected from visitors to our websites, and usage information relating to the operation of the Services (together, "Business Operations Data", as further described in our Data Processing Addendum). This Policy governs that processing.
- Parta.io as processor. Where Parta.io provides the Services to an organization (for example, your employer) under an agreement with that organization, Parta.io processes personal information contained in Customer Content on behalf of, and under the instructions of, that organization, which acts as the controller of such data. Such processing is governed by our agreement with that organization, including our Data Processing Addendum (the "DPA"), and not by this Policy. If your personal information is contained in Customer Content, please direct privacy inquiries to the relevant organization, and we will support it in responding to your request.

This Policy does not apply to third-party applications or services that integrate with our Services, or to any other third-party products, services or businesses.

Please read this Policy carefully. If you have any questions about how we process your personal information, please contact us as described in the "Contacting Us" section below.

1. Information We Collect

We collect the following categories of information: (1) information that you provide to us directly; (2) information that is collected automatically when you use the Services; and (3) information that we receive from third parties.

A. Information You Provide to Us

Registration and Account Information

When you register for an account to access or use our Services (an "**Account**"), we ask for and may collect personal information that can be used to identify you, such as your name, email address, phone number,

physical address, job title, organization name, and online identifiers, together with billing and transaction information where you purchase the Services ("**Personal Information**").

We do not knowingly collect special categories of personal data (such as data concerning health, biometric or genetic data, racial or ethnic origin, political opinions, or religious or philosophical beliefs) or other sensitive personal information through the Services, and we ask that you do not submit such information to us.

Communications

If you contact us directly — for example, for customer support or sales inquiries — we collect the contents of your message and any information you choose to provide.

B. Information Collected Automatically

We and our service providers may automatically collect certain information whenever you access or interact with the Services ("**Usage Data**"). Usage Data may include the browser and operating system you are using, the URL that referred you to the Services, the areas within the Services that you visited, the links you clicked, the pages or content you viewed and for how long, content response times, download errors, the length of visits to certain pages, and similar information commonly shared when browsers communicate with websites. We may combine Usage Data with other information we collect about you in order to provide, secure and improve the Services and for analytics purposes.

Usage Data includes your IP address, which is a number assigned to your device whenever you access the internet. IP addresses may be recorded for IT security and system diagnostic purposes, and may be used in aggregate form to maintain and improve the Services and to generate and analyze statistics about the use of the Services.

We use the following technologies to collect Usage Data:

Cookies

Cookies are small text files placed on your device to collect standard internet log information and visitor behavior information. We use the following categories of cookies:

- Strictly necessary cookies, which are required for the operation of the Services (for example, authentication and security cookies);
- Functional cookies, which remember your preferences and settings; and
- Analytics cookies, which help us understand how visitors interact with the Services so that we can improve them.

Where required by applicable law (including in the European Economic Area and the United Kingdom), we obtain your consent before placing cookies other than strictly necessary cookies, and you may withdraw or adjust your consent at any time through the cookie settings made available on our websites. You can also set your web browser to refuse all cookies or to indicate when a cookie is being sent; however, some features of the Services may not function properly if the ability to accept cookies is disabled. Where information collected through cookies constitutes Personal Information under applicable law, we treat it in accordance with this Policy.

Web Beacons

A web beacon is a small image file on a web page or in an email that can be used to collect certain information from your device, such as an IP address, the time the content was viewed, a browser type, and the existence of cookies previously set by the same server. Web beacons or similar technologies may be used to count visitors to our Services, to monitor how Users navigate the Services, or to measure whether emails we send have been opened.

C. Information from Third Parties

We may provide an option to access or register for the Services through credentials you use for certain services provided by third parties (each, a "Third-Party Service"), such as your Google account. By authorizing us to connect with a Third-Party Service, you authorize Parta.io to access and store the information that the Third-Party Service makes available to us, and to use and disclose it in accordance with this Policy. It is your responsibility to review the privacy settings, terms of use and privacy policy of such Third-Party Services to control what information is made available to us.

We may also receive your business contact information from your organization when it provisions your access to the Services.

Third-Party Services also include artificial intelligence model providers and AI agents that you or your organization choose to connect to the Services, whether through an API integration or through the Model Context Protocol, as further described in Section 4 (Artificial Intelligence Features and Connected AI Agents) below. Parta.io does not operate such providers and agents, and their processing of your information is governed by their own terms and privacy policies.

2. How We Use Information; Legal Bases

We use the information we collect for the purposes set out in the table below. Where the EU or UK General Data Protection Regulation ("GDPR") applies, the table also identifies the legal bases on which we rely.

Purpose	Categories of Personal Information	Legal Basis (where GDPR applies)
Creating and administering your Account; providing, operating and maintaining the Services; processing transactions; providing customer support	Registration Data; billing and transaction information; communications with us	Performance of a contract with you or with your organization; our legitimate interest in administering and delivering the Services
Securing the Services; preventing fraud and abuse; monitoring compliance with our agreements and policies	Registration Data; Usage Data; log and device information	Our legitimate interests in protecting the Services, our Users and our business; compliance with legal obligations
Improving and developing the Services; analytics; understanding how the Services are used	Usage Data; aggregated or de-identified information	Our legitimate interests in improving the Services; consent, where required for non-essential cookies and similar technologies

Sending service-related notices and administrative communications	Registration Data; contact information	Performance of a contract; our legitimate interests in communicating with Users about the Services
Sending marketing and promotional communications about our Services; promoting and marketing the Services	Contact information; marketing preferences	Consent, where required by applicable law; otherwise, our legitimate interest in promoting the Services to business contacts
Delivering AI-powered features that you or your organization choose to use, as described in Section 4	Content you choose to submit to AI features; related configuration settings	Performance of a contract; your direction and, where applicable, consent
Complying with legal obligations; establishing, exercising or defending legal claims	Any of the categories described in this Policy, as relevant	Compliance with legal obligations; our legitimate interests in protecting our legal rights

Where we rely on your consent to process Personal Information, you have the right to withdraw your consent at any time. Withdrawal does not affect the lawfulness of processing based on consent before its withdrawal. Where we rely on legitimate interests not already described in this Policy, we will make clear to you at the relevant time what those interests are. If you have any questions about the legal bases on which we collect and use your Personal Information, please contact us as described in the "Contacting Us" section below.

We may also aggregate or de-identify information such that it no longer reasonably identifies you, and use such information for any lawful purpose, including to monitor, develop and improve the Services. We will not attempt to re-identify de-identified information, except as permitted by applicable law (for example, to test the effectiveness of our de-identification processes).

3. How We Share Information

No Sale or Sharing of Personal Information

We do not sell Personal Information, and we do not share Personal Information for cross-context behavioral advertising, as those terms are defined under applicable US state privacy laws, and we have not done so in the preceding twelve (12) months. We do not use or disclose sensitive personal information for purposes other than those permitted by applicable law. We also do not permit our service providers to use the Personal Information that we share with them for their own marketing purposes or for any purpose other than performing services for us.

Service Providers and Subprocessors

We share information, including Personal Information, with third-party service providers that perform services on our behalf, such as hosting, infrastructure, analytics, payment processing, customer relationship management, communications and support. These providers may access or process your Personal Information only for the purpose of providing these services to us, on our behalf and in accordance with our instructions. We will retain control over and remain responsible for your Personal Information and will use

appropriate safeguards, as required by applicable law, to ensure its integrity and security when engaging such providers.

Where Parta.io processes Customer Personal Data on behalf of an organization, the subprocessors authorized to process such data — including the identity of AI Subprocessors — are identified in the Subprocessor List set out in Exhibit 3 to our Data Processing Addendum, which forms part of our agreement with that organization and is updated in accordance with the DPA. The DPA also describes the controller-side providers that we use to process Business Operations Data for our own purposes.

Connected AI Providers and AI Agents

Where you or your organization connect an artificial intelligence model or AI agent to the Services, content is transmitted to that provider at your direction and on your behalf, as described in Section 4 (Artificial Intelligence Features and Connected AI Agents). Such transmissions are initiated by you, not by Parta.io, and are governed by your (or your organization's) agreement with that provider.

Compliance with Law; Protection of Rights

We may share your Personal Information with courts, law enforcement authorities, regulators, attorneys or other parties where it is reasonably necessary for the establishment, exercise or defense of a legal claim, for a confidential alternative dispute resolution process, or where we believe disclosure is necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or violations of our Terms, or as otherwise required by applicable law, regulation, judicial or official request.

Corporate Transactions

We may share your Personal Information with any third party to whom we assign or novate any of our rights or obligations, or that acquires all or substantially all of our business, stock or assets, or with whom we merge. In such an event, we will require the recipient to honor the commitments made in this Policy and will notify you, as required by applicable law, before your Personal Information becomes subject to a materially different privacy policy.

With Your Consent

We will otherwise disclose your Personal Information only when you direct us to do so or otherwise give us your permission.

4. Artificial Intelligence Features and Connected AI Agents

A. Our Approach to AI

Parta.io does not develop, train, or host its own artificial intelligence models. AI-powered functionality available in the Services operates through third-party AI model providers and AI agents that you or your organization choose to connect ("**Connected AI Providers**"). You may connect a Connected AI Provider in two ways: (i) through an API integration configured by you or your organization, or (ii) by connecting an MCP-compatible AI agent through our Model Context Protocol server ("**Parta MCP**"). Where the Services include built-in AI functionality for which no provider selection is available, such functionality is provided using third-party AI model providers that we engage as AI Subprocessors under enterprise terms that prohibit the use of your content to train models, consistent with Section 5 of our Data Processing Addendum. The third parties we engage in providing the Services, including AI Subprocessors, are identified in our Data Processing Addendum.

AI features may include, depending on your plan and configuration: generating or improving draft content (rewriting, simplifying, summarizing, expanding, or adjusting the tone of text); grammar and style checking; translating and localizing learning content into other languages; converting source materials you provide into structured drafts (for example, turning documents into a course outline or course draft); and AI-assisted authoring workflows through connected agents.

All AI features are optional and disabled unless you or your organization choose to use them. Functionality that relies on AI is clearly indicated by corresponding labels in the Services, and your organization's administrators can enable or restrict AI functionality for their workspace.

We do not use your content or Personal Information to train any artificial intelligence models, and we do not permit Connected AI Providers to be engaged by us for that purpose, consistent with Section 5 of our Data Processing Addendum. Whether a Connected AI Provider uses data submitted to it for model training is determined by the terms of your (or your organization's) own agreement with that provider.

B. AI Features via API

When you or your organization connect an AI model through an API integration, content that you choose to process with AI features is transmitted to the Connected AI Provider for processing at your direction. Parta.io limits such transmission to the data needed to fulfill the requested action — the text you select or input, your prompt or instruction, applicable generation settings, and, where relevant, limited surrounding context. Parta.io does not use such content for any purpose other than delivering the requested feature. The Connected AI Provider's processing of that content — including its storage, retention, and any use for model improvement — is governed by that provider's own terms and privacy policy, which we encourage you to review before connecting a provider.

AI-generated results are returned to you as editable drafts: they are not published or applied automatically, and you review, edit, regenerate, or discard them before use. AI outputs are accessible only to authorized users within your workspace; we do not share your AI inputs or outputs with other customers, and your data is logically segregated from the data of other customers.

C. AI Agents via Parta MCP

Parta MCP is a server based on the open Model Context Protocol that allows an MCP-compatible AI agent to read and modify content in your Parta authoring environment at your direction. When you use Parta MCP:

- Parta.io does not receive, store, or have access to the contents of your conversations with the AI agent, other than any content that the agent includes in a tool-call payload at your direction. The Parta MCP server receives only tool-call payloads — that is, which action the agent requested and with what parameters.
- Tool-call payloads are logged for debugging and security purposes and are stored alongside our backend logs, accessible only to authorized Parta.io engineering personnel. Such logs are retained for no more than three (3) months. Logged payloads that contain Customer Personal Data are processed as such under our Data Processing Addendum, including its return and deletion obligations.
- Authentication uses OAuth 2.0 with Dynamic Client Registration. Access and refresh tokens are stored on the client side; Parta.io stores only token hashes and the client identifier. When you select "Forget this app," the client identifier is revoked and all associated tokens expire immediately.
- An AI agent connected through Parta MCP can act only within the permissions of the Parta account used to authorize the connection, consistent with the role and permission model of the Services. Connections

are established by individual users through OAuth authorization, and the agent acts on that user's behalf. Organization administrators do not manage individual agent connections directly; however, deactivating a user's account immediately revokes the access of any AI agent connected through that account.

- All Parta MCP traffic is encrypted in transit, and data at rest within our infrastructure is encrypted, as part of the security measures applicable to the Services and described in Exhibit 2 to our Data Processing Addendum.

D. Your Choices and Responsibilities

The decision to connect an AI model or AI agent, and the choice of provider, rests with you or your organization. Before submitting content containing Personal Information to AI features or an AI agent, please ensure that such use is consistent with your organization's policies and applicable law. Parta.io does not control, and is not responsible for, the privacy practices of Connected AI Providers. You may disconnect a Connected AI Provider or revoke an AI agent connection at any time in the applicable settings, and your organization's administrator may terminate an agent's access by deactivating the associated user account.

Parta.io's AI features are designed as content-creation and authoring tools. They are not intended to make automated decisions that produce legal or similarly significant effects concerning individuals, and we do not use your Personal Information for automated decision-making of that kind. If the nature of our AI functionality materially changes, we will update this Policy in accordance with the section "Changes to This Privacy Policy" below.

Upon termination of your (or your organization's) agreement with us, content processed through AI features — including AI inputs and outputs stored in your workspace — can be exported and will be deleted in accordance with the applicable agreement (including Section 12 of the Data Processing Addendum, where applicable) and Section 5 (How Long We Retain Your Personal Information).

5. How Long We Retain Your Personal Information

We retain your Personal Information for as long as is needed to fulfill the purposes outlined in this Policy, unless a longer retention period is required or permitted by law (for example, for tax, accounting or other legal requirements). To determine the appropriate retention period, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process it and whether we can achieve those purposes through other means, and applicable legal requirements.

When we have no ongoing legitimate business need to process your Personal Information, we will either delete or anonymize it, or, if this is not possible (for example, because your Personal Information has been stored in backup archives), we will securely store your Personal Information and isolate it from any further processing until deletion is possible.

For Customer Personal Data that we process on behalf of an organization, we retain and delete such data in accordance with our agreement with that organization, including Section 12 (Return and Deletion of Customer Personal Data) of our Data Processing Addendum, subject to applicable law.

6. Your Privacy Rights

Users may update or change their Account information by editing their profile within the Services.

Depending on your location and subject to applicable law, you may have the right to: (i) access the Personal Information we hold about you and receive a copy of it in a portable format; (ii) correct inaccurate Personal Information; (iii) request deletion of your Personal Information; (iv) restrict or object to certain processing of your Personal Information; and (v) withdraw your consent at any time where processing is based on consent, without affecting the lawfulness of processing carried out before such withdrawal.

To exercise these rights, please contact us as described in the "Contacting Us" section below. We will respond to your request within the timeframe required by applicable law. If we extend the response period where permitted by applicable law, we will notify you of the extension and the reasons for it. To protect your privacy and security, we may take reasonable steps to verify your identity before acting on a request. Please note that, notwithstanding a deletion request, certain information may be retained as needed to provide you with the Services, comply with our legal obligations, resolve disputes and enforce our agreements.

If your Personal Information is contained in Customer Content that we process on behalf of an organization, we will refer your request to that organization and support it in responding, in accordance with our Data Processing Addendum.

Objections to Processing

Where we process your Personal Information on the basis of our legitimate interests, you have the right to object to such processing on grounds relating to your particular situation. We will honor your objection unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or the processing is necessary for the establishment, exercise or defense of legal claims. Where we process your Personal Information for direct marketing purposes, you may object at any time, and we will stop such processing. You may also lodge a complaint with your local data protection supervisory authority.

7. US State Privacy Rights

This Section supplements the rest of this Policy and applies to residents of US states with comprehensive privacy laws — including the California Consumer Privacy Act, as amended by the California Privacy Rights Act (the "**CCPA**"), and the comprehensive privacy laws of Virginia, Colorado, Connecticut, Utah, Texas, Oregon and other states, in each case to the extent such laws apply to us and to the processing of your Personal Information (collectively, "**US State Privacy Laws**").

Categories of Personal Information

In the preceding twelve (12) months, we have collected the categories of Personal Information described in Section 1 (Information We Collect), which correspond to the following statutory categories: identifiers (such as name, email address, phone number and online identifiers); customer records information (such as billing information); professional or employment-related information (such as job title and organization); commercial information (such as records of Services purchased); and internet or other electronic network activity information (such as Usage Data). We collect these categories from the sources, for the purposes, and share them with the categories of recipients, described in Sections 1 through 3 of this Policy. We retain each category as described in Section 5.

No Sale or Sharing; Sensitive Personal Information

We do not sell Personal Information and we do not share Personal Information for cross-context behavioral advertising, and we have not done so in the preceding twelve (12) months. We do not knowingly sell or share the Personal Information of consumers under 16 years of age. We do not collect or process sensitive personal

information for the purpose of inferring characteristics about you, and we do not use or disclose sensitive personal information for purposes that would require a right to limit under US State Privacy Laws. Because we do not sell or share Personal Information, opt-out preference signals such as the Global Privacy Control do not change how we process your Personal Information; where required by law, we will nevertheless treat such signals as a valid request to opt out of any sale or sharing.

Your Rights

Subject to applicable law and certain exceptions, you have the right to:

- **Know / Access:** request that we disclose the categories and specific pieces of Personal Information we have collected about you, the categories of sources, the purposes for collection, and the categories of third parties to whom we disclose Personal Information, and to receive a copy of your Personal Information in a portable format;
- **Correct:** request that we correct inaccurate Personal Information that we maintain about you;
- **Delete:** request that we delete Personal Information that we collected from you, subject to the exceptions set out in US State Privacy Laws (for example, where retention is necessary to complete a transaction, detect security incidents, debug the Services, exercise or defend legal claims, or comply with a legal obligation);
- **Opt out:** opt out of the sale or sharing of Personal Information and of targeted advertising (noting that we do not engage in these activities); and
- **Non-discrimination:** not receive discriminatory treatment for exercising your privacy rights. We will not deny you the Services, charge you a different price, or provide a different level or quality of the Services because you exercised your rights under US State Privacy Laws.

Exercising Your Rights

To exercise the rights described above, please submit a request to us at support@parta.io. Only you, or someone legally authorized to act on your behalf, may make a request related to your Personal Information. If you use an authorized agent, we may require proof of the agent's authority and may verify your identity directly. Your request must provide sufficient information to allow us to reasonably verify that you are the person about whom we collected Personal Information (which may include your first name, last name, the email address used to register with Parta.io, and phone number) and describe your request with sufficient detail to allow us to understand, evaluate and respond to it.

We cannot respond to your request or provide you with Personal Information if we cannot verify your identity or authority to make the request. Making a request does not require you to create an Account with us; however, we consider requests made through your password-protected Account sufficiently verified when the request relates to Personal Information associated with that Account. We will only use Personal Information provided in a request to verify the requestor's identity or authority to make the request. We will respond within the timeframes required by applicable law. If we decline to take action on your request, you may have the right to appeal our decision by replying to our response with the subject line "Appeal", and we will inform you of the outcome of your appeal as required by applicable law.

California "Shine the Light"

California Civil Code Section 1798.83 permits California residents to request certain information regarding disclosure of personal information to third parties for their direct marketing purposes. We do not disclose Personal Information to third parties for their direct marketing purposes.

8. Children's Privacy

The Services are intended for business use and are not directed to individuals under the age of sixteen (16). We do not knowingly collect Personal Information from individuals under 16. If we become aware that we have inadvertently received Personal Information from an individual under the age of 16, we will delete such information from our records. If you believe that we may have collected Personal Information from an individual under 16, please contact us as described in the "Contacting Us" section below.

9. Security

We take the security of your Personal Information seriously and use appropriate technical and organizational measures designed to protect it against unauthorized or unlawful processing and against accidental loss, destruction or damage. These measures include encryption of data in transit and at rest, access controls, and logical segregation of customer data, and are further described in Exhibit 2 (Technical and Organizational Security Measures) to our Data Processing Addendum. While no method of transmission or storage is completely secure, we regularly review and update our security practices. For more information about our security program, please contact us as described in the "Contacting Us" section below.

10. International Data Transfers

We may transfer, store and process your Personal Information in the United States and in other countries whose data protection laws may differ from those of your country of residence. Where we transfer Personal Information originating from the European Economic Area, the United Kingdom or Switzerland to a country that has not been recognized as providing an adequate level of data protection, we implement appropriate safeguards required by applicable law, such as the Standard Contractual Clauses approved by the European Commission (and their UK equivalent), as further described in Section 10 of our Data Processing Addendum where it applies. You may request a copy of the relevant safeguards by contacting us as described in the "Contacting Us" section below.

11. Changes to This Privacy Policy

We may update this Policy from time to time. If we do, we will post the revised Policy on our website with an updated "Last Updated" date. If we make material changes to this Policy, we will notify you before the changes take effect — for example, by sending an email to the address associated with your Account or by posting a prominent notice within the Services — and, where required by applicable law, we will obtain your consent. We encourage you to review this Policy periodically to stay informed about our privacy practices.

12. Contacting Us

If you have any questions regarding this Policy or the information we hold about you, or if you wish to exercise any of your rights, you may contact us at:

Parta IO Corp.

16192 Coastal Highway

Lewes, Delaware 19958, USA

Email: support@parta.io

In order for us to take the appropriate action, please describe in reasonable detail the nature of your request or inquiry.