MYNT

PRIVACY POLICY

How Mynt collects, uses, shares, protects, and deletes personal data

Operator	Pyvot Consultancy & Analytics Private Limited
Effective date	28 July 2026
Website	https://pyvot.in
Published at	https://pyvot.in/privacy

Contact: contact@pyvot.in | +91 98366 66745

PRIVACY AT A GLANCE
Mynt collects and processes information needed to provide an AI-powered productivity platform. Google Sign-In provides basic profile information, and the optional Gmail integration is read-only. Google user data is used only for user-facing features, is not sold or used for advertising, and is not used to train general-purpose AI or machine-learning models. Anyone may submit a data-deletion request through Mynt's public deletion page without signing in; requests are verified before deletion is carried out.

1. Who we are and scope of this Policy

This Privacy Policy describes how Pyvot Consultancy & Analytics Private Limited ("Pyvot", "Mynt", "we", "us", or "our") processes personal data through the Mynt website, web and mobile applications, integrations, customer support, communications, and related services (collectively, the "Service").

Our registered office is at 3rd Floor, Unit 303, Arch Square, X2, Block EP & GP, Salt Lake, Sector V, North 24 Parganas, West Bengal 700091, India. For privacy questions or requests, contact contact@pyvot.in.

This Policy applies to individual users, business customers, authorised workspace users, website visitors, and people who communicate with us. It does not govern independent processing by third-party websites, services, or customer organisations.

2. Our role

For account, website, billing, support, security, and product-operation information, Mynt generally acts as the entity determining why and how personal data is processed.

For Customer Data submitted to a business workspace, the business customer may determine the purposes and means of processing and Mynt may act on its instructions. In that case, users should also review the organisation's privacy notices and direct organisation-specific requests to its administrator.

3. Information we collect

3.1 Account and profile information

When you create or manage an account, we may collect your name, email address, phone number, organisation, role, profile details, account settings, and authentication information. If you use Google Sign-In, Google may provide your name, email address, profile image, and Google account identifier as shown on the consent screen.

3.2 Gmail data

If you separately connect Gmail, Mynt may receive read-only access to the Gmail data covered by the exact scope displayed on Google's consent screen. Depending on that scope and the feature you use, this may include message metadata, sender and recipient information, subject lines, message bodies, threads, labels, and attachments.

Mynt does not use the Gmail read permission to send, modify, move, label, archive, or delete messages. We access Gmail data only after you authorise the connection and only to provide the user-facing feature you request.

3.3 Content you provide

We collect prompts, instructions, files, spreadsheets, text, images, reports, feedback, configurations, and other content that you upload, paste, enter, or generate through the Service. Uploaded files and spreadsheets are user-provided content; the current Google integration does not request Google Drive or Google Sheets access.

3.4 Usage, device, and technical information

We may collect device type, operating system, browser type, app version, language, approximate location derived from IP address, IP address, timestamps, pages or features used, performance data, diagnostic logs, crash information, security events, and identifiers used for authentication, fraud prevention, and analytics.

3.5 Payment and transaction information

For paid plans, we collect subscription details, billing contact information, invoices, payment status, tax information, and transaction references. Payments are processed by Razorpay. Mynt generally does not receive or store full card or bank credentials entered directly into Razorpay's payment interface.

3.6 Communications

We collect information you provide when you contact us by email, telephone, support channels, or WhatsApp, including the content of the communication and related contact details. We may also record your communication preferences and delivery status for reports and notices.

3.7 Information from organisations and other users

A business customer or workspace administrator may provide information about authorised users, assign roles, upload Customer Data, or direct us to create or manage accounts. Other users may include information about you in files, emails, reports, or shared workspace content.

4. How we use information

We use personal data for the following purposes:

- create, authenticate, administer, and secure accounts;
- provide, personalise, maintain, troubleshoot, and support the Service;
- process user-requested AI features, including summarising email, analysing uploaded files or spreadsheets, extracting information, and preparing reports or insights;
- provide Google Sign-In and the optional read-only Gmail integration;
- deliver reports and communications by email or WhatsApp at your request or according to settings you choose;
- process subscriptions, payments, invoices, taxes, renewals, cancellations, and fraud checks;
- monitor performance, diagnose errors, prevent abuse, protect users, and maintain security;
- analyse product usage and improve the reliability, usability, and functionality of the Service without using private customer content or Google user data to train general-purpose AI models;
- respond to enquiries, requests, complaints, and legal claims;
- comply with legal, regulatory, accounting, tax, and contractual obligations; and
- send promotional communications where permitted, with an option to unsubscribe.

5. Google user data: access, use, storage, and sharing

5.1 Permissions requested

Mynt requests only the Google permissions needed for features you choose to use. The production Service uses Google Sign-In and may request read-only Gmail access. The exact data and permissions are displayed on Google's consent screen before access is granted.

5.2 Purpose and user benefit

Google Sign-In is used to authenticate your account and populate basic profile information. Gmail data is used only to provide visible productivity features you request, such as searching or summarising email, extracting tasks, dates, amounts, or other information, and generating reports or insights for you.

5.3 No automatic connected-account actions

Mynt does not send emails or take other actions in your connected Google Account through the Gmail read permission. Any Service action that could affect an external account must be initiated or expressly approved by you and must use a separately authorised permission.

5.4 Limited Use and prohibited uses

Mynt's use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. In particular:

- Google user data is used only to provide or improve the user-facing feature for which you granted access;
- Google user data is not sold, rented, or transferred to data brokers;
- Google user data is not used for advertising, retargeting, personalised marketing, surveillance, credit decisions, lending, or unrelated profiling;
- Google Workspace APIs and Google user data are not used to develop, improve, or train general-purpose or non-personalised AI or machine-learning models;
- Google user data is not combined with analytics data for advertising purposes; and
- human access to Google user data is limited to cases where you give specific consent, access is necessary for security or abuse investigation, access is required by law, or access is strictly necessary to provide support you request.

5.5 AI processing of Google data

When you request an AI feature involving Gmail data, Mynt may transmit the minimum necessary email content to a contracted third-party AI processing provider. The provider acts on our instructions solely to generate the result you requested and is contractually restricted from using the content to train its own general-purpose models or for unrelated purposes.

5.6 Revoking access

You can disconnect Google through Mynt settings where available or revoke Mynt's access from your Google Account's third-party access controls. Revocation invalidates or disables the relevant access token and may stop connected features from working. You may also request deletion through our public Data Deletion Request page at https://pyvot.in/data-deletion or by contacting contact@pyvot.in.

6. AI processing

Mynt may use contracted third-party AI processing providers to process prompts, Gmail content, files, spreadsheets, and other content only when necessary to provide an AI feature you request. We limit the information sent to what is reasonably necessary for the task.

Customer data, private User Content, and Google user data will not be used by Mynt or its contracted AI providers to train general-purpose AI or machine-learning models. We may use aggregated or de-identified operational information that does not reasonably identify a person or reveal customer content to improve performance, reliability, and security.

AI-generated results may contain errors. Review the Terms of Service for important limitations regarding AI Output.

7. Legal grounds and permitted purposes

Depending on the applicable law and context, we process personal data based on one or more of the following: your consent; performance of a contract or steps requested before entering a contract; compliance with legal obligations; legitimate uses or interests such as security, support, fraud prevention, and service improvement; and the establishment, exercise, or defence of legal claims.

Where processing is based on consent, you may withdraw consent at any time. Withdrawal does not affect processing that was lawful before withdrawal and may prevent a feature from functioning.

8. How we share information

We do not sell or rent personal data. We may disclose information to the following recipients only as necessary for the purposes described in this Policy:

- Amazon Web Services (AWS), for cloud hosting, infrastructure, storage, security, and related operations;
- contracted third-party AI processing providers, for user-requested AI features under processing and no-training restrictions;
- Razorpay, for payment processing, subscriptions, fraud prevention, refunds required by law, and payment support;
- Google, for Google Sign-In, Gmail authorisation, email-delivery infrastructure, Firebase Analytics where enabled, and Google Play app analytics where enabled;
- WhatsApp and its service providers, when you choose or configure communication or report delivery through WhatsApp;
- professional advisers such as lawyers, auditors, accountants, insurers, and consultants under confidentiality duties;
- business customers and workspace administrators where your account belongs to their organisation;
- courts, regulators, law-enforcement agencies, government bodies, or other parties when disclosure is required by law or reasonably necessary to protect rights, safety, and security; and
- a buyer, investor, affiliate, or successor in connection with a merger, financing, reorganisation, acquisition, or sale of all or part of the business, subject to applicable legal requirements.

We do not send Gmail content, uploaded files, or spreadsheet content to Firebase Analytics, Google Play analytics, Razorpay, or WhatsApp unless you expressly direct the relevant content to be delivered through WhatsApp. Google user data is not shared for advertising or general analytics.

9. Analytics, cookies, and similar technologies

The website and applications may use essential cookies, local storage, and similar technologies for authentication, preferences, security, load balancing, and core functionality.

Where enabled, Firebase Analytics may be used for web or application usage analytics, and Google Play analytics may provide app-installation, performance, and crash information. We configure analytics to avoid collecting Gmail message content, uploaded file contents, spreadsheet contents, or other private customer content. Consent controls will be used where required by law.

You can control cookies through browser or device settings, although disabling essential technologies may affect the Service.

10. Data retention and deletion

10.1 General rule

We retain personal data only for as long as reasonably necessary to provide the Service, fulfil the purposes described in this Policy, comply with legal and contractual obligations, resolve disputes, and enforce agreements.

10.2 Public data deletion requests and account deletion

You may request deletion of your Mynt account and associated personal data through our public Data Deletion Request page at https://pyvot.in/data-deletion. The page is publicly accessible and does not require you to sign in. You can submit the email address associated with your Mynt account or data, and the request will be recorded for review by authorised Mynt administrators. You may also submit a deletion request by emailing contact@pyvot.in. For

security, submitting an email address does not itself trigger automatic deletion. We may verify that you control the submitted email address and may request additional information reasonably necessary to confirm identity, authority, and the scope of the request. This is intended to prevent unauthorised or fraudulent deletion requests. Once a valid request is verified, we will delete or de-identify the applicable account and associated personal data within thirty (30) days, except for information that must be retained for legal, security, fraud-prevention, dispute, tax, accounting, or other lawful purposes. We may retain a limited record of the deletion request and its disposition where reasonably necessary to demonstrate compliance or prevent abuse.

10.3 Backups

Deleted information may remain in encrypted or access-restricted backups for up to ninety (90) days before being overwritten or removed through normal backup cycles. Backup data is not restored for ordinary business use after a valid deletion request, except where necessary for disaster recovery, security, or legal compliance.

10.4 Google access tokens and Gmail data

Google access and refresh tokens are retained only while needed to maintain the connection and are invalidated, deleted, or rendered unusable when you disconnect Google, revoke access, the token expires, or the Mynt account is deleted.

Gmail data is processed on demand or temporarily as needed to provide the requested feature. If an email-derived summary, report, or extracted item is saved to your account, it is retained as User Content until you delete it or close the account. Gmail data and saved derivatives subject to an account deletion request are deleted within thirty (30) days, with backup copies expiring within ninety (90) days.

10.5 Financial, security, and support records

Invoices, tax records, transaction references, and related financial records are retained for the period required by applicable law. Security logs, abuse-prevention records, support communications, and legal records are retained for as long as reasonably necessary for the relevant purpose and then deleted or de-identified.

11. International processing

Mynt is based in India and uses service providers that may process information in India and other countries where they or their subprocessors operate. Those countries may have different data-protection laws.

Where required, we use contractual, organisational, and technical safeguards for cross-border processing and comply with applicable restrictions on transferring personal data.

12. Security

We use reasonable administrative, technical, and organisational safeguards designed to protect personal data. These measures may include access controls, authentication, encryption in transit, encryption at rest where appropriate, logging, monitoring, backup controls, vulnerability management, personnel confidentiality obligations, and vendor due diligence.

Access to private customer content and Google user data is restricted to authorised personnel and service providers with a legitimate need and appropriate obligations. No system is completely secure, and we cannot guarantee absolute security.

If you believe your account or information has been compromised, contact contact@pyvot.in promptly. Do not use the public deletion form to report urgent security incidents.

13. Your choices and rights

Subject to applicable law and verification of your request, you may have the right to:

- access information about the personal data we process and obtain a copy where applicable;
- correct, complete, or update inaccurate personal data;
- request deletion of personal data;
- withdraw consent and disconnect Google or other integrations;
- object to or request restriction of certain processing where applicable;
- request portability of information where applicable;
- opt out of promotional communications;
- nominate another person to exercise rights in circumstances recognised by applicable Indian law; and
- raise a grievance with us and, where available, complain to the competent data-protection authority.

To exercise a data-deletion right, use our public Data Deletion Request page at https://pyvot.in/data-deletion or email contact@pyvot.in. For other privacy rights, you may email contact@pyvot.in from the address associated with your account and describe the request. We may ask for information reasonably necessary to verify identity, authority, and scope before acting on a request. We will respond within the period required by applicable law.

14. Business workspaces

If you use Mynt through an organisation, the organisation may control your workspace account and Customer Data. Its administrators may be able to manage access, view or export workspace information, set retention rules, and delete accounts or content.

Mynt processes organisation-controlled Customer Data in accordance with the customer agreement and lawful instructions. An organisation's internal processing is governed by its own notices and policies.

15. Children's privacy

The Service is intended for users aged eighteen (18) or older. We do not knowingly permit children to create accounts or knowingly collect personal data from children through the Service. If you believe a child has provided personal data, contact us so that we can investigate and delete it where appropriate.

16. Third-party services and links

The Service may contain links to or integrations with third-party services. Those third parties process information under their own terms and privacy policies. This Policy does not control their independent practices, including practices of Google, Razorpay, WhatsApp, app stores, or websites you choose to access.

17. Changes to this Policy

We may update this Policy to reflect changes in law, technology, vendors, features, or data practices. We will publish the updated version at https://pyvot.in/privacy and revise the "Last updated" date.

If a change materially affects how we use Google user data or other personal data, we will provide prominent notice and obtain consent where required before applying the new use.

18. Grievance Officer and contact details

For privacy questions, account deletion, data-rights requests, security concerns, or grievances, contact:

Organisation	Pyvot Consultancy & Analytics Private Limited
Grievance Officer	Sanchit Surana, Grievance Officer

Email	contact@pyvot.in
Phone	+91 98366 66745
Address	3rd Floor, Unit 303, Arch Square, X2, Block EP & GP, Salt Lake, Sector V, North 24 Parganas, West Bengal 700091, India
Website	https://pyvot.in

Schedule A — Google Data Access Summary

This Schedule summarises the Google data currently requested by Mynt and the related user-facing purpose.

Google access	Data involved	Purpose	Actions permitted	Retention
Google Sign-In	Name, email, profile image, Google account identifier	Authenticate the user and create or populate the Mynt profile	Sign in only	Retained with the Mynt account until deletion; backups may persist up to 90 days
Gmail read-only	Message metadata, senders and recipients, subjects, bodies, threads, labels, and attachments within the authorised scope	Search or summarise email, extract user-requested information, and prepare productivity reports or insights	Read only; no send, edit, move, label, archive, or delete permission	Processed on demand or temporarily; saved outputs remain until deleted; account deletion within 30 days and backup expiry within 90 days

Uploaded files and spreadsheets are provided directly by users and are not accessed through Google Drive or Google Sheets permissions under the current configuration.

Effective date: 28 July 2026 | Last updated: 29 July 2026