

PRIVACY POLICY

Privacy Notice

Dividend Portfolio Planner

Document control	Value
Document owner	Dividend Portfolio Planner
Effective date	September 3, 2026
Version	1.0
Review cycle	At least annually and after material legal, product, vendor, or data-processing changes
Classification	Public

Policy objective: Explain what personal data Dividend Portfolio Planner (DPP) collects, how DPP uses and protects that information, how long information is retained, when information may be shared, and the privacy rights and choices available to users.

Trust Center note: This is a public, user-facing privacy notice derived from DPP's Data Privacy, Retention and Deletion Policy. It does not disclose confidential internal controls, personal information, or sensitive security procedures.

1. Purpose and scope

This Privacy Policy describes how DPP handles personal information associated with the DPP website, applications, accounts, subscriptions, support services, research and portfolio-planning features, analytics, communications, and related services (collectively, the “Platform”).

It applies to personal data DPP collects directly from users, receives through authorized service providers, or generates through use of the Platform. Different or additional notices may apply where required by law or for a specific service.

2. Privacy principles

DPP's privacy program is based on the following principles:

- Purpose limitation: use personal data for documented, legitimate, and communicated purposes.
- Data minimization: collect and retain only information reasonably necessary for those purposes.
- Storage limitation: delete or de-identify information when its purpose and required retention period end.
- Accuracy and integrity: maintain reasonable processes to correct materially inaccurate information.
- Least privilege: restrict access according to role and business need.
- Security and accountability: protect information throughout its lifecycle and maintain evidence of material privacy decisions.

- User rights: support applicable access, correction, export, deletion, restriction, objection, consent-withdrawal, and opt-out rights.
- Vendor accountability: oversee service providers that process DPP information on DPP's behalf.

3. Personal data we collect

The information DPP collects depends on how a user interacts with the Platform. DPP's internal privacy policy identifies the following principal categories.

Category	Examples	Why it may be collected
Account and identity data	Account identifiers, contact information, authentication records, consent and preference records.	Create and administer accounts, authenticate users, communicate with users, maintain preferences, and protect accounts.
Portfolio and planning data	User-entered portfolio holdings, ticker selections, watchlists, scenarios, backtests, assumptions, saved calculations, and exports.	Provide DPP's educational, research, comparison, portfolio-planning, and analytical features.
Subscription and transaction data	Subscription status, invoices, transaction and refund records, and payment-related metadata.	Administer subscriptions, billing, accounting, tax, customer service, and transaction records.
Support and communications	Customer support communications and information a user chooses to provide when requesting assistance.	Respond to requests, troubleshoot issues, maintain service records, and improve support.
Usage, device, network, and analytics data	Application activity, technical logs, device or browser information, network information, analytics events, and similar identifiers.	Operate, secure, troubleshoot, measure, and improve the Platform.
Cookie and preference data	Cookie identifiers, browser-storage values, consent choices, and similar technologies as configured.	Maintain sessions and preferences, protect the Platform, remember privacy choices, and support permitted analytics or marketing functions.
Security information	Authentication events, security logs, incident information, fraud indicators, and other information necessary to protect DPP and users.	Prevent, detect, investigate, and respond to unauthorized access, abuse, fraud, and security incidents.

4. Information DPP seeks to minimize

DPP seeks to avoid collecting information that is not reasonably necessary for the Platform or another documented business, security, legal, support, billing, or analytical purpose.

DPP's internal policy states that full payment-card numbers and card security codes should not be stored by DPP and that card processing should be performed through an approved hosted payment processor.

Users should not provide passwords, authentication codes, full payment-card information, highly sensitive personal information, or other unnecessary confidential information through support messages, free-text fields, or other areas not designed for that information.

5. How DPP uses personal data

DPP may use personal data for the following purposes, as applicable to the user's interaction with the Platform:

- Provide, operate, maintain, and improve DPP services.
- Create, authenticate, secure, and administer user accounts.
- Provide portfolio-planning, research, scenario, backtesting, calculation, and related educational functionality.
- Process and administer subscriptions, transactions, invoices, refunds, and related records.
- Respond to customer-support requests and service communications.
- Maintain user preferences, consent choices, and privacy selections.
- Monitor Platform performance, diagnose errors, and improve functionality.
- Protect DPP, users, and service providers against fraud, abuse, unauthorized access, and security threats.
- Comply with applicable legal, tax, accounting, contractual, audit, dispute, and recordkeeping obligations.
- Conduct analytics or marketing activities where appropriately disclosed and subject to applicable choices or consent requirements.

6. Data minimization, analytics, AI, and new uses

DPP reviews new tracking, profiling, advertising, artificial intelligence, data-enrichment, material data-sharing, and similar uses for privacy and security considerations before activation.

DPP's internal policy prohibits using production personal data in development, testing, screenshots, prompts, or demonstrations unless expressly approved and suitably masked or protected.

DPP seeks to avoid unnecessary local downloads and duplicate exports containing personal data and to remove them when the authorized task is complete.

7. How personal data may be shared

DPP may disclose personal data to service providers and other recipients where reasonably necessary for an authorized purpose. Depending on the services DPP uses, these recipients may include providers supporting cloud infrastructure, authentication, payment processing, communications, analytics, market data, software development, security, or customer support.

DPP's vendor-management requirements call for appropriate due diligence and contractual safeguards addressing authorized processing, security, incident notification, privacy-request assistance, retention, return, and deletion.

DPP may also preserve or disclose information where reasonably necessary to comply with applicable law, respond to valid legal process, investigate fraud or security incidents, protect legal rights, resolve disputes, or satisfy other lawful obligations.

The source policies do not identify the specific production vendors currently used by DPP. Where DPP publishes a subprocessor or service-provider list, that list should be maintained separately and kept current.

8. Cookies and browser storage

DPP may use cookies, local storage, session storage, and similar browser technologies for functions such as authentication, security, preferences, consent choices, Platform performance, and analytics.

Users should review the DPP Cookie Policy for additional information about the categories of cookies and browser storage DPP may use and how to control or remove them.

9. Data retention

DPP retains information only for as long as reasonably necessary for the applicable purpose, subject to legal, accounting, security, dispute, fraud-prevention, contractual, and other documented requirements.

DPP's Data Privacy, Retention and Deletion Policy establishes the following operational defaults, which may be adjusted where a different legally or contractually required period applies.

Record category	DPP operational retention default
Active account profile and preferences	For the life of the active account; delete or de-identify after verified closure, subject to permitted exceptions.
Portfolio inputs, scenarios, watchlists, backtests, and saved analyses	For the life of the active account; active-system deletion generally within 30 days after verified deletion or closure.
Incomplete registration and temporary verification data	Generally 30 days after abandonment or expiration.
Subscription, invoice, tax, refund, and transaction records	Generally seven years after transaction or account closure, unless a different period is approved.
Customer support communications	Generally three years after case closure, unless needed for a dispute, fraud matter, or legal hold.
Consent, notice, privacy-request, and opt-out evidence	Generally five years after the event or request closes, with minimal suppression evidence retained where required.
Marketing records	Until withdrawal or inactivity, then generally up to 24 months; minimum do-not-contact information may be retained as necessary.
Routine application and technical logs	Generally up to 12 months.
Authentication and security logs	Generally up to 24 months.
Security incident and investigation records	Generally seven years after closure or as otherwise directed for legal or security purposes.
Cookies and similar identifiers	For the disclosed lifespan; nonessential identifiers generally no longer than 13 months under the current internal default.
Temporary files, caches, and exports	For operational need only, normally no longer than 30 days.
Backup copies	Under an approved rotation, generally no longer than 90 days.

Where multiple retention requirements apply, DPP's internal policy calls for retaining the record for the longest documented required period and recording the basis. Irreversibly anonymized or aggregate information may be retained while useful where re-identification is not reasonably possible.

10. Account deletion and deletion requests

Users may request account deletion or exercise applicable deletion rights through the privacy, support, web, email, or in-application method DPP makes available.

DPP's internal process calls for verifying the requester as appropriate, determining the scope and applicable legal requirements, identifying relevant active systems and processors, and deleting or irreversibly de-identifying covered information.

For covered portfolio and account data, active-system deletion is generally targeted within 30 days after verified approval, or sooner where required by applicable law.

Deletion from protected backup copies may occur through normal backup expiration where the backups are encrypted, access-restricted, unavailable for ordinary use, and not used to circumvent a valid deletion request.

11. Information DPP may retain after a deletion request

DPP may retain limited information when reasonably necessary to:

- Complete a requested transaction.
- Meet tax, accounting, contractual, or recordkeeping obligations.
- Maintain security and prevent fraud.
- Exercise, establish, or defend legal claims.
- Comply with a legal hold, subpoena, investigation, audit, regulatory inquiry, or government requirement.
- Maintain a suppression or do-not-contact record.
- Demonstrate that DPP properly handled a privacy request.

Information retained for an exception is restricted to the applicable purpose and should be deleted when the exception ends.

12. Security

DPP maintains administrative, technical, and organizational safeguards designed to protect information throughout its lifecycle. The source policies identify controls including data classification, encryption, role-based access, multifactor authentication for privileged access, secure software-development practices, logging and monitoring, incident response, backup and recovery, and third-party oversight.

No security program can guarantee absolute security. Users should protect their credentials and promptly report suspected unauthorized account access.

Additional information is available in the DPP Information Security Overview and Access Control Policy.

13. Your privacy rights

Depending on the user's location and applicable law, a user may have rights concerning personal data. DPP's internal privacy policy is designed to support applicable rights including:

- Access: request information about personal data DPP maintains about you.
- Correction: request correction of materially inaccurate personal data.
- Export or portability: request a copy of applicable personal data in a usable form where required.
- Deletion: request deletion of applicable personal data, subject to lawful exceptions.
- Restriction: request limits on certain processing where applicable.
- Objection: object to certain processing where applicable.
- Consent withdrawal: withdraw consent for processing that relies on consent, without affecting prior lawful processing.
- Opt out: exercise applicable opt-out rights, including marketing or other processing choices where required.

The availability and scope of a particular right depend on the law that applies to the user and the processing activity.

14. How to exercise your rights

DPP should provide a designated in-application, web, email, or support method for privacy requests. Requests may require reasonable identity verification to protect users against unauthorized disclosure, account takeover, and social engineering.

DPP's process is designed to avoid requesting unnecessary new personal data solely for verification. Where an authorized agent is permitted by law, DPP may verify the agent's authority and the requester's identity as appropriate.

DPP will evaluate applicable deadlines, exceptions, extensions, and response requirements based on the relevant law and circumstances.

15. Marketing and communications choices

Where DPP sends optional marketing communications, users may withdraw or change applicable marketing preferences through the methods DPP provides. DPP may retain minimum suppression information necessary to honor a do-not-contact request.

Service, security, account, transaction, or legal communications may still be sent where necessary to provide or protect the Platform or comply with applicable obligations.

16. Third-party services and links

DPP may integrate with or link to third-party services. A third party's own collection and use of information may be governed by its privacy notice and terms.

Users should review applicable third-party privacy practices when choosing to use an external service. DPP's oversight responsibilities apply to providers processing DPP information on DPP's behalf as described in DPP's internal policies and applicable contracts.

17. International processing

DPP's supplied internal policy materials contemplate data locations and cross-system transfers as part of DPP's data inventory and vendor oversight, but they do not identify the specific countries in which DPP currently processes personal data.

If DPP processes personal data across jurisdictions, DPP should use applicable safeguards and update this public Privacy Policy or related Trust Center materials as necessary to describe material international processing and legally required transfer mechanisms.

18. Children's privacy

The supplied DPP privacy and security policies do not establish a specific minimum age for use of the Platform. DPP's Terms & Conditions of Use should define account eligibility before publication of a definitive children's-privacy statement.

DPP should not knowingly collect personal data from children in a manner inconsistent with applicable law.

19. Changes to this Privacy Policy

DPP may update this Privacy Policy to reflect changes in Platform functionality, data practices, service providers, legal requirements, or privacy and security controls.

The current version will identify its effective date. Material changes may be communicated through the Platform or other reasonable means where appropriate.

20. Related Trust Center documents

Document	Purpose
Data Privacy, Retention and Deletion Policy	Provides additional detail on DPP's data lifecycle, retention, deletion, privacy-request, backup, and processor practices.
Information Security Overview	Provides a public overview of DPP's information security program.
Access Control Policy	Describes DPP's authorization, authentication, access-management, and access-review practices.
Cookie Policy	Explains cookies, browser storage, and user controls.

Data Processing Addendum	Describes processor commitments for applicable team and business customers.
Acceptable Use Policy	Defines permitted and prohibited uses of DPP.
Terms & Conditions of Use	Establishes contractual terms governing use of the Platform.

21. Contact

Questions about this Privacy Policy or requests concerning personal data may be submitted through the official privacy, support, or contact methods published on the Dividend Portfolio Planner website or Trust Center.

Users should not include passwords, authentication codes, full payment-card information, or other unnecessary sensitive information in privacy or support communications.

TRUST CENTER NOTICE

This Privacy Policy is intended to provide users with a clear public description of DPP's personal-data practices. DPP should keep this notice aligned with the Platform's actual production configuration, service providers, account eligibility rules, privacy-request channels, and legally required disclosures.