

DATA PROCESSING ADDENDUM

Team and Business Customers

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, privacy, product, vendor, or data-processing changes
Classification	Public

Document objective: Establish the data-processing commitments that apply when an organization purchases or administers DPP services for multiple users and DPP processes personal data on that organization's behalf.

Implementation note: This public template is designed for DPP team or business customers. The existing DPP policy materials do not identify DPP's current production subprocessors, international transfer mechanism, legal entity name, or customer-specific processing instructions. Those items must be completed and verified before this Addendum is offered for execution.

1. Purpose and relationship to the agreement

This Data Processing Addendum (DPA) supplements the agreement governing a team, business, enterprise, or other organizational customer's use of Dividend Portfolio Planner (DPP) services (the "Agreement"). It applies to the extent DPP processes Customer Personal Data on behalf of the customer in connection with the services.

If this DPA conflicts with the Agreement regarding processing of Customer Personal Data, this DPA controls to the extent of that conflict. Capitalized terms not defined here have the meaning given in the Agreement.

2. Definitions

For this DPA:

- "Customer" means the organization that has entered into the Agreement for DPP services.
- "Customer Personal Data" means personal information or personal data processed by DPP on behalf of Customer through the services.
- "Data Protection Laws" means privacy and data-protection laws applicable to the processing covered by this DPA, including, where applicable, the GDPR and U.S. state privacy laws such as the CCPA/CPRA.

- “GDPR” means Regulation (EU) 2016/679 and, where applicable, substantially equivalent United Kingdom data-protection requirements.
- “CCPA” means the California Consumer Privacy Act, as amended by the California Privacy Rights Act and implementing regulations, to the extent applicable.
- “Process,” “processing,” “controller,” “processor,” “business,” “service provider,” “consumer,” and similar terms have the meanings assigned by applicable Data Protection Laws.
- “Subprocessor” means a third party engaged by DPP to process Customer Personal Data on DPP's behalf in providing the services.

3. Roles of the parties

The parties acknowledge that their privacy roles depend on the processing activity and applicable law.

For Customer Personal Data that DPP processes solely on Customer's documented instructions, Customer acts as controller or business and DPP acts as processor or service provider/contractor, as those terms are applicable.

Customer is responsible for determining the lawfulness of its instructions, providing required notices, establishing an appropriate legal basis, and obtaining any required permissions or consents for Customer Personal Data submitted to DPP.

DPP may process certain information for its own legitimate operational, security, billing, legal-compliance, fraud-prevention, or service-administration purposes where DPP acts independently under applicable law. Such processing is governed by applicable DPP privacy notices and policies rather than by Customer's processor instructions.

4. Customer processing instructions

DPP will process Customer Personal Data only on documented instructions from Customer, including instructions contained in the Agreement, this DPA, Customer's authorized configuration and use of the services, and other mutually agreed written instructions, unless processing is required by applicable law.

If DPP is legally required to process Customer Personal Data other than on Customer's instructions, DPP will inform Customer before processing unless applicable law prohibits that notice.

DPP will notify Customer if, in DPP's reasonable view, a Customer instruction infringes applicable Data Protection Laws, subject to applicable legal restrictions.

5. GDPR processor commitments

To the extent GDPR processor obligations apply, DPP will:

- Process Customer Personal Data only on documented Customer instructions, subject to applicable law.
- Ensure persons authorized to process Customer Personal Data are subject to appropriate confidentiality obligations.

- Implement appropriate technical and organizational measures designed to protect Customer Personal Data, taking into account the nature, scope, context, and purposes of processing and relevant risks.
- Engage subprocessors in accordance with Section 9 and impose appropriate data-protection obligations on them.
- Taking into account the nature of processing, reasonably assist Customer with appropriate technical and organizational measures for responding to requests by data subjects.
- Reasonably assist Customer with applicable security, personal-data-breach, data-protection impact assessment, and prior-consultation obligations, taking into account the nature of processing and information available to DPP.
- At the end of the applicable services, delete or return Customer Personal Data as provided in Section 12, unless applicable law requires retention.
- Make information reasonably necessary to demonstrate compliance with applicable processor obligations available to Customer and support audits in accordance with Section 13.

6. CCPA/CPRA service-provider and contractor commitments

To the extent DPP processes Personal Information for Customer as a service provider or contractor under the CCPA, DPP will process that Personal Information for the specific business purposes described in the Agreement, this DPA, and Customer's documented instructions.

Subject to the CCPA's definitions, exceptions, and permitted business purposes, DPP will not:

- Sell Customer Personal Information.
- Share Customer Personal Information for cross-context behavioral advertising.
- Retain, use, or disclose Customer Personal Information outside the direct business relationship with Customer except as permitted by applicable law.
- Retain, use, or disclose Customer Personal Information for a commercial purpose other than the business purposes specified in the Agreement or as otherwise permitted by applicable law.
- Combine Customer Personal Information received from or on behalf of Customer with Personal Information received from another person or collected from DPP's own interactions with a consumer, except where permitted by applicable law.

DPP will provide the same level of privacy protection required of applicable service providers or contractors under the CCPA, will notify Customer if DPP determines it can no longer meet applicable obligations, and will permit Customer to take reasonable and appropriate steps to help ensure that Customer Personal Information is used consistently with Customer's CCPA obligations.

7. Confidentiality and security

DPP maintains an information security program designed to protect the confidentiality, integrity, and availability of information entrusted to the Platform. Security practices include risk-based safeguards, access controls, authentication protections, secure software-development practices, vulnerability

management, logging and monitoring, incident response, backup and recovery practices, and third-party oversight.

Additional public information is available in the DPP Information Security Overview and Access Control Policy. DPP's internal security documentation may contain confidential operational information and is not incorporated into this public DPA unless expressly agreed.

8. Personal data breach

DPP will notify Customer without undue delay after becoming aware of a confirmed Personal Data Breach affecting Customer Personal Data where notification is required by applicable Data Protection Laws.

To the extent reasonably available and legally permitted, notice will include information appropriate to help Customer understand the nature of the incident, affected information, known or reasonably anticipated consequences, and mitigation or remediation actions.

DPP's notification of an incident is not an admission of fault or liability. Customer remains responsible for determining its own notification or reporting obligations as controller/business.

9. Subprocessors

9.1 Authorization

Customer provides general authorization for DPP to engage subprocessors necessary to provide, secure, support, analyze, or maintain the services, subject to this Section.

DPP will require subprocessors that process Customer Personal Data to enter into written obligations providing data-protection safeguards appropriate to the processing and applicable law. DPP remains responsible for its subprocessor obligations to the extent required by applicable Data Protection Laws.

9.2 Subprocessor changes

DPP should maintain a current public subprocessor list and provide reasonable notice of material additions or replacements where required by applicable law or contract. Customer may raise a reasonable data-protection objection to a new subprocessor within the period specified in the Agreement or applicable notice.

The parties will work in good faith to address a valid objection. If no commercially reasonable alternative is available, the Agreement should specify the parties' rights regarding the affected service.

9.3 Current subprocessor list

The DPP policy materials supplied for preparation of this DPA identify categories of providers—such as cloud, authentication, payment, analytics, email/SMS, market-data, code-repository, and other technology providers—but do not identify the specific production vendors currently used by DPP. Accordingly, no vendor names are invented in this document.

Subprocessor	Service / purpose	Data categories	Processing location	Status
[To be verified and published]	Cloud hosting / infrastructure	As applicable to hosted DPP data	[Verify]	Complete before publication
[To be verified and published]	Authentication / identity	Account and authentication data	[Verify]	Complete before publication
[To be verified and published]	Payment processing	Subscription and payment-related metadata; DPP policy states full card numbers/security codes should not be stored by DPP	[Verify]	Complete before publication
[To be verified and published]	Analytics / performance	Usage, device/browser, analytics information as configured	[Verify]	Complete before publication
[To be verified and published]	Email / communications	Contact and service-communication data	[Verify]	Complete before publication
[To be verified and published]	Market data / external integrations	Data necessary for applicable service integration	[Verify]	Complete before publication

Before Trust Center publication, DPP should replace this placeholder table with the verified production subprocessor list, including the provider's legal name, purpose, relevant data categories, and primary processing location where appropriate.

10. Data subject and consumer requests

Taking into account the nature of processing, DPP will provide reasonable assistance to Customer in responding to applicable requests concerning Customer Personal Data, such as access, correction, deletion, portability, restriction, objection, or opt-out rights, where Customer cannot reasonably fulfill the request through available DPP functionality.

If DPP receives a request directly from an individual concerning Customer Personal Data for which Customer is the controller/business, DPP may direct the individual to Customer unless applicable law requires DPP to respond directly.

Customer is responsible for verifying the requester's identity and determining whether and how a request must be fulfilled, except to the extent applicable law assigns that responsibility to DPP.

11. International data transfers

If Customer Personal Data subject to GDPR transfer restrictions is transferred to a country that has not been recognized as providing an adequate level of protection, the parties will use an applicable lawful transfer mechanism.

The supplied DPP materials do not establish DPP's current international transfer locations or mechanism. Before offering this DPA to customers subject to GDPR transfer restrictions, DPP should

identify applicable processing locations and implement the appropriate mechanism, which may include applicable Standard Contractual Clauses and required supplementary measures.

Where Standard Contractual Clauses are used, the parties should complete the required modules, annexes, competent supervisory authority, governing-law selections, and transfer details applicable to the actual relationship.

12. Return, deletion, and retention

At the end of services involving Customer Personal Data, DPP will delete or return Customer Personal Data in accordance with the Agreement, Customer's documented instructions, DPP's Data Privacy, Retention and Deletion Policy, and applicable law.

DPP may retain limited information where reasonably necessary for legal, tax, accounting, security, fraud-prevention, dispute, legal-hold, suppression, or compliance purposes. Any retained information will remain subject to appropriate protections and will be used only for the applicable retention purpose.

Backup copies may expire through normal protected backup rotation where permitted by applicable law and are not to be used to circumvent a valid deletion requirement.

13. Compliance information and audits

Upon reasonable request and subject to appropriate confidentiality and security protections, DPP will make information reasonably necessary to demonstrate compliance with applicable processor obligations available to Customer.

Where legally required and not reasonably satisfied by available documentation, DPP will allow and contribute to a reasonable audit by Customer or an independent auditor appointed by Customer, subject to reasonable advance notice, scope, frequency, confidentiality, security, and non-disruption requirements.

The parties may agree that current independent assessments, certifications, security documentation, questionnaires, or similar assurance materials satisfy all or part of an audit request where appropriate.

14. Processing details

Processing detail	Description
Subject matter	Provision, administration, security, support, and operation of DPP services for Customer.
Duration	For the term of the Agreement and any limited retention period permitted or required under the Agreement, this DPA, or applicable law.
Nature and purpose	Hosting and operating accounts; providing portfolio-planning, research, analytical and related service functionality; authentication; support; security; subscription administration; and other documented Customer-directed

	processing.
Categories of data subjects	Customer-authorized users, administrators, representatives, and other individuals whose Customer Personal Data is submitted to or generated through Customer's authorized use of DPP.
Types of Customer Personal Data	Account and identity/contact information; authentication-related information; user-entered portfolio holdings, ticker selections, watchlists, scenarios, backtests, assumptions and saved calculations; subscription/support information; and usage, device, network, analytics, and security information as applicable to the services.
Special categories / sensitive data	DPP is not designed for Customer to submit special-category or highly sensitive personal data unless expressly supported and agreed. Customer should not submit unnecessary sensitive information.
Frequency	Continuous or as initiated by Customer and authorized users during use of the services.

15. Customer responsibilities

Customer will:

- Use the services and provide processing instructions in compliance with applicable Data Protection Laws.
- Provide required privacy notices and establish an appropriate legal basis for Customer Personal Data.
- Limit Customer Personal Data submitted to DPP to information reasonably necessary for the services.
- Configure access appropriately and manage authorized users.
- Respond to data-subject or consumer requests for which Customer is responsible.
- Not instruct DPP to process data in a manner that violates applicable law.

16. Related Trust Center documents

Document	Purpose
Data Privacy, Retention and Deletion Policy	Describes DPP's privacy, retention, deletion, processor, and privacy-request practices.
Information Security Overview	Provides a public overview of DPP's security program.
Access Control Policy	Describes DPP's authorization, authentication, access-management, and review controls.
Cookie Policy	Explains DPP's cookies, browser storage, and user controls.
Acceptable Use Policy	Defines permitted and prohibited uses of DPP.
Terms & Conditions of Use	Establishes contractual terms governing use of DPP.

17. Order of precedence and changes

This DPA may be updated to reflect changes in Data Protection Laws, DPP services, subprocessors, or processing practices. Material changes affecting Customer's processor relationship should be handled in accordance with the Agreement and applicable law.

Customer-specific negotiated terms, executed Standard Contractual Clauses, or other legally required data-transfer terms control over this public template to the extent of a conflict.

18. Execution and contact

This public DPA template is intended to support team and business customers. Before execution, the parties should identify the contracting legal entities, effective date, Agreement, and any customer-specific processing or transfer terms.

Privacy and DPA questions may be submitted through the official 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 communications.

TRUST CENTER NOTICE

This Data Processing Addendum is a public template describing DPP's intended processor commitments for organizational customers. It is not a representation that GDPR, CCPA/CPRA, international-transfer requirements, or any other law applies to every customer or processing activity. Customer-specific applicability and execution requirements should be reviewed before use.