PLANFUL DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement (the "**Agreement**") is made between Planful, Inc. ("**Planful**") and ("**Client**") (collectively the "**Parties**").

1. **Subject Matter and Duration.**

   a) **Subject Matter.** This DPA reflects the Parties' commitment to abide by Applicable Data Protection Laws (defined below) concerning the Processing of Client Personal Data in connection with Planful's execution of the Agreement. All capitalized terms that are not expressly defined in this Data Processing Addendum will have the meanings given to them in the Agreement. If and to the extent language in this DPA or any of its exhibit's conflicts with the Agreement, this DPA shall control.

   b) **Duration and Survival.** This DPA will become legally binding upon the Effective Date of the Agreement or upon the date that the Parties sign this DPA if it is completed after the effective date of the Agreement. Planful will Process Client Personal Data until the relationship terminates as specified in the Agreement. Planful's obligations and Client's rights under this DPA will continue in effect until the later of: (a) the date on which Planful has completed all data return or deletion obligations under Section 8 or one hundred twenty (120) days after the expiration or termination of the Agreement. For the avoidance of doubt, this DPA will automatically terminate on the date determined under Section 1(b), regardless of whether any Client Personal Data remains in Planful's possession due to legal or regulatory retention requirements, provided that Planful shall continue to protect any such retained Client Personal Data in accordance with Section 8(b).

2. **Definitions**. For the purposes of this DPA, the following terms and those defined within the body of this DPA apply.

   a) "**Applicable Data Protection Law(s)**" means the Applicable Data Protection Law(s) both international and domestic to the United States including, as applicable including but not limited to: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (iii) the Swiss Federal Act on Data Protection ("FADP"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

   b) "**Client Personal Data**" means Personal Data Processed by Planful pertaining to Client's business and related to individuals whose Personal Data is subject to Applicable Data Protection Laws. The Client Personal Data and the specific uses of the Client Personal Data are detailed in Exhibit A attached hereto.

   c) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

   d) "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

   e) "**Planful Account Data**" means Personal Data that relates to Planful's relationship with Client, including but not limited to, the names or contact information of individuals Client has associated with its account. Planful Account Data also includes any data Planful may need to collect for the purpose of managing its relationship with Client, identity verification, or as otherwise required by applicable laws and regulations.

   f) "**Planful Usage Data**" means Services usage data and configuration metrics collected and processed by Planful in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

g) "**Process**" or "**Processing**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

h) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Client Personal Data on behalf of Client subject to this DPA.

i) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful loss, unauthorized disclosure of, or access to Client Personal Data Processed by Planful. Security Incident does not include (a) unsuccessful access attempts, including pings, port scans, denial-of-service attacks, or other network-level attacks on firewalls or networked systems that do not result in unauthorized access to Client Personal Data; or (b) unsuccessful login attempts, brute-force password attacks, or similar events that do not compromise the security of Client Personal Data.

j) "**Sell**", and "**Share**" shall have the same meanings as set forth under Applicable Data Protection Law(s) US.

k) "**Services**" means any and all services that Planful performs under the Agreement, including Application Services.

l) "**Service Provider**" shall have the same meanings as set forth under Applicable Data Protection Law(s) US.

m) "**Swiss DPA**" means the Swiss Standard Contractual Clauses DPA as set out in Exhibit E of this DPA.

n) "**Third Party(ies)**" means Planful's authorized contractors, agents, vendors and third-party service providers (i.e., sub-processors) that Process Client Personal Data.

o) "**UK DPA**" means the International Data Transfer DPA to the EU Commission Standard Contractual Clauses set out in Exhibit D of this DPA.

3. Data Use and Processing.

a) Roles of the Parties. The parties acknowledge and agree that with regard to the processing of Personal Data, Client may act either as a Controller or Processor and, except as expressly set forth in this DPA or the Agreement, Planful is a Processor. Where Client acts as a Processor on behalf of a third-party Controller, Client warrants that: (i) it has obtained all necessary authorizations from the relevant Controller(s) to appoint Planful as a sub-processor; (ii) it has obtained all necessary authorizations to permit Planful's use of Third Parties in accordance with Section 3(d); and (iii) Client's instructions to Planful, including those regarding the transfer of Client Personal Data, have been authorized by the relevant Controller(s). Client shall indemnify and hold Planful harmless from any claims, losses, or liabilities arising from Client's failure to obtain such authorizations.

b) Compliance with Laws. Client Personal Data shall be Processed in compliance with the terms of this DPA and all Applicable Data Protection Law(s).

c) Documented Instructions; Processing of Personal Data. Planful and its Third Parties shall Process Client Personal Data only in accordance with the documented instructions of Client or as specifically authorized by this DPA, the Agreement, or any applicable Statement of Work. Planful will, unless legally prohibited from doing so, inform Client in writing if it reasonably believes that there is a conflict between Client's instructions and applicable law or otherwise seeks to Process Client Personal Data in a manner that is inconsistent with Client's instructions. Client shall ensure that Planful's processing of Personal Data in accordance with Client's instructions will not cause Planful to be in breach of the Applicable Data Protection Law(s). Client is solely responsible for the accuracy, quality, and legality of (i) the Client Personal Data provided to Planful by or on behalf of Client, (ii) the means by which Client acquired any such Client Personal Data, and (iii) the instructions it provides to Planful regarding the processing of such Client Personal Data. Client shall not provide or make available to Planful any Client Personal Data in violation of the Agreement or Applicable Data Protection Law(s).

d) Authorization to Use Third Parties. To the extent necessary to fulfill Planful's contractual obligations under the Agreement or any Statement of Work, Client hereby authorizes (i) Planful to engage Third Parties and (ii)

Third Parties to engage sub-processors. Any Third-Party Processing of Client Personal Data shall be consistent with Client's documented instructions and comply with all Applicable Data Protection Law(s). Client consents to Planful appointing sub-processors listed in Exhibit C and https://planful.com/sub-processors/. Planful may update the sub-processor list from time to time. Planful agrees that any updates to the Sub-Processor list will take effect prior to such new sub-processor having access to Client Data. Planful shall notify Client of any changes to this list if the Client signs up for notices through the Sub-Processor URL. Following such notice period, Client has 10 days to object on reasonable grounds to the use of such sub-processor. Following such notice, the Parties agree to work in good faith on resolving any objections to the use of sub-processors by Planful.

e) Planful and Third-Party Compliance. Planful agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties' Processing of Client Personal Data that imposes on such Third Parties (and their sub-processors) data protection and security requirements for Client Personal Data that are compliant with Applicable Data Protection Law(s) and are substantially similar to those set out in this Agreement; and (ii) remain responsible to Client for Planful's Third Parties' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Client Personal Data.

f) Confidentiality. Any person or Third Party authorized to Process Client Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.

g) Personal Data Inquiries and Requests. Planful agrees to comply with all reasonable instructions from Client related to any requests from individuals exercising their rights in Client Personal Data granted to them under Applicable Data Protection Law(s) ("Privacy Request"). To the extent permitted by law, Planful will notify Client of a Privacy Request without undue delay. If Planful receives a Privacy Request in relation to Client Data, Planful shall direct the data subject to submit their request to Client. Client will be responsible for responding to such request. Client is solely responsible for ensuring that Privacy Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Client Personal Data are communicated to Planful, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each data subject. To the extent Client is unable to respond to Privacy Requests without Planful's assistance, Planful will use commercially reasonable measures to assist Client in answering or complying with any Privacy Request in so far as it is possible and without undue delay. Such assistance shall be provided at Client's expense. To the extent that the assistance required exceeds the capabilities of the Application Services' standard functionality, Planful may charge its then-current professional services rates for such assistance.

h) Data Protection Impact Assessment and Prior Consultation. Planful agrees to provide reasonable assistance at Client's expense to Client where, in Client's judgement, the type of Processing performed by Planful is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

i) Demonstrable Compliance. Planful agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide any necessary records to Client to demonstrate compliance upon reasonable request.

j) Selling and Sharing of Personal Data. Client agrees that with the exceptions of Planful Account Data and Planful Usage Data, Planful is a Service Provider and is receiving Client Personal Data from Client in order to provide Services pursuant to the Agreement, which constitutes a business purpose under Applicable Data Protection Law(s) US. Planful will not (i) Sell or Share Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than the specific purpose of performing its obligations under the Agreement, including retaining, using, or disclosing the Personal Data for a commercial purpose other than fulfilling its obligations under the Agreement; or (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Client and Planful.

k) Compliance Management. Planful will promptly notify Client in writing in the event that it determines it is no

longer able to meet its obligations under Applicable Data Protection Law(s) or this DPA. Planful shall take appropriate measures to remediate its noncompliant Processing of Personal Data.

l) Planful's Role as a Controller. The parties agree that with respect to Planful Usage Data and Planful Account Data, Planful is an independent Controller, and the parties are not joint Controllers. Planful will process Planful Usage Data and Planful Account Data solely to (i) manage the relationship with Client, including but not limited to performing its obligations to Client under the Agreement; (ii) to carry out Planful's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Client; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Planful is subject; and (vi) as otherwise permitted or required under Applicable Data Protection Law(s) and in accordance with this DPA and the Agreement.

4. Cross-Border Transfers of Personal Data.

a) Cross-Border Transfers of Personal Data. Client authorizes Planful and its Third Parties to transfer Client Personal Data across international borders, including from the European Economic Area to the United States. Any cross-border transfer of Client Personal Data must be supported by an approved adequacy mechanism.

b) Standard Contractual Clauses. Planful and Client will use the Standard Contractual Clauses in Exhibit B as the adequacy mechanism supporting the transfer and Processing of Client Personal Data.

c) Transfer Impact Assessments. Planful has conducted Transfer Impact Assessments for all countries outside of Europe where Planful transfers Personal Data. Planful will review and, as necessary, re-evaluate the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data outside of Europe.

5. Information Security Program.

a) Planful agrees to implement appropriate technical and organizational measures designed to protect Client Personal Data as required by Applicable Data Protection Law(s) and as outlined in the Information Security Addendum (the "**Information Security Program**"). Such measures shall include:

i) Pseudonymisation of Client Personal Data where appropriate, and encryption of Client Personal Data in transit and at rest;

ii) The ability to ensure ongoing confidentiality, integrity, availability of Planful's Processing and Client Personal Data;

iii) The ability to restore the availability and access to Client Personal Data in the event of a physical or technical incident; and

iv) A process for regularly evaluating and testing the effectiveness of Planful's Information Security Program to ensure the security of Client Personal Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Planful's Information Security Program shall be consistent with the objectives set forth in SOC 2 Type II (or a substantially equivalent successor standard). Planful shall make its most recent SOC 2 Type II report available to Client upon written request, subject to Planful's reasonable confidentiality requirements. Planful shall not materially diminish the protections of its Information Security Program during the term of this DPA. Technical and organizational security measures currently implemented by Planful are described in Annex II.

6. Security Incidents.

a) Security Incident Procedure. Planful will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects and remediate the cause to extent within Planful's reasonable control, and (ii) reasonably restore the availability or access to Client Personal Data in a timely manner.

b) Notice. Planful agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) (but in no event longer than seventy-two (72) hours) to Client's Designated POC if it knows that a Security Incident has taken place. Such notice will include all reasonably available details required for Client to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident. Planful's notification of a Security Incident shall not be construed as an acknowledgment of fault or liability with respect to such incident

c) Confidentiality of Security Incidents. Client shall not publicly disclose the details of any Security Incident, including the nature, scope, root cause, or remediation measures, without Planful's prior written consent, except to the extent such disclosure is (i) required by Applicable Data Protection Laws or a regulatory authority, or (ii) necessary to comply with Client's own notification obligations to affected data subjects under Applicable Data Protection Laws. Where disclosure is required by law, Client shall, to the extent permitted by applicable law, provide Planful with reasonable advance notice and an opportunity to review and comment on the proposed disclosure. The parties shall cooperate in good faith regarding the content and timing of any required public disclosures related to a Security Incident.

7. Client Obligations.

a) Client is responsible for reviewing the information made available by Planful relating to data security and making an independent determination as to whether the Services meets Client's requirements and legal obligations under the applicable Data Protection Laws.

b) Client is solely responsible for complying with Security Incident notification laws applicable to Client and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

8. Data Storage and Deletion.

a) Data Storage. Planful will not store or retain any Client Personal Data except as necessary to perform the Services under the Agreement.

b) Data Deletion. Upon expiration or termination of the Agreement, at Client's written request made within twenty-eight (28) days after such termination or expiration, Planful will provide Client with temporary access to the Planful platform to retrieve Client Personal Data in a commercially standard, machine-readable format (e.g., CSV or similar). If Client requires Planful to perform data extraction beyond the standard export functionality of the Application Services, such extraction shall be provided at Client's expense at Planful's then-current professional services rates. If Client does not submit a written request for data retrieval within the twenty-eight (28) day period, Planful will permanently delete or destroy all Client Personal Data in its possession or control, except to the extent retention is required by applicable law. Audits.

9. Audits. During the term of this Agreement, Planful shall, upon Client's written request, make available to Client Planful's most recent SOC 2 Type II audit report (or equivalent successor certification) and such additional information as is reasonably necessary to demonstrate Planful's compliance with its obligations under this DPA and Applicable Data Protection Laws, provided that Planful shall have no obligation to disclose commercially confidential information, proprietary source code, or information relating to other Planful customers.

a) On-Site Audits. Client may conduct or commission an on-site audit of Planful's facilities and practices relevant to the Processing of Client Personal Data, subject to the following conditions:

i) Client may exercise this right no more than once in any twelve (12) month period, unless (A) a Security Incident affecting Client Personal Data has occurred, (B) Client is required to conduct an audit by a regulatory or supervisory authority with jurisdiction over Client, or (C) Planful's most recent SOC 2 Type II report reveals a material deficiency relevant to Client Personal Data;

ii) Client shall provide Planful with no less than thirty (30) days' prior written notice of an audit request, including the proposed scope, duration, and identity of any third-party auditor;

iii) the audit shall be limited in scope to matters reasonably required for Client to assess Planful's compliance with this DPA and the parties' compliance with Applicable Data Protection Law(s);

iv) audits shall be conducted during Planful's regular business hours in a manner that minimizes disruption to Planful's operations;

v) all audits shall be at Client's sole expense, and shall occur at a date and time mutually agreed by the parties;

vi) any third-party auditor engaged by Client shall be bound by confidentiality obligations no less protective than those set forth in the Agreement and shall not be a competitor of Planful; and

b) SOC 2 Safe Harbor. To the extent that Client's audit objectives can be satisfied by review of Planful's most recent SOC 2 Type II report, such review shall be deemed to satisfy Client's audit rights under this Section 8 for the period covered by the report. This safe harbor does not apply in the circumstances described in Section 8(b)(i)(A) through (C) above.

10. Data Processing Locations.

a) Planful's primary data processing and storage locations for Client Personal Data are set forth in Exhibit C (or, where specified, in the applicable Order Form). Client Personal Data shall be Processed and stored in the locations specified in the applicable Order Form or, if no location is specified, in the locations set forth in Exhibit C.

b) Planful shall provide Client with not less than thirty (30) days' prior written notice before materially changing the location from which Client Personal Data is Processed or stored.

c) Client acknowledges that certain support, maintenance, and administrative activities may involve access to Client Personal Data from locations other than the primary processing locations specified in Exhibit C. Such access locations are identified in Exhibit C alongside the applicable sub-processors.

11. Miscellaneous.

a) Liability. Planful's aggregate liability arising out of or relating to this DPA, including liability for Security Incidents, fines and penalties imposed by a government agency, and claims brought against Client by third parties relating to Planful's breach of its obligations under this DPA, shall be subject to the Limitation of Liability clause set forth in the Agreement.

b) Counterparts. This DPA may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this DPA delivered by facsimile, e-mail or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this DPA. The parties have caused this DPA to be executed by their respective authorized representatives, as of the date indicated below the representative's signature.

c) The Agreement. All other terms and conditions in the Agreement shall remain in full force and effect.

12. Contact Information.

a) Planful and the Client agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

- Planful Designated POC: dpo@planful.com
- Client Designated POC: As set forth in the Order Form

[Signature Page to Follow]

planful

Exhibit A

Client Personal Data

1.1 Subject Matter of Processing	The Processing will involve Processing for data and application integration services. The subject matter of Processing is the Services pursuant to the Master Subscription Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Master Subscription Agreement.
1.3 Categories of Data Subjects	Includes the following: ● Prospects, Clients, business partners and vendors of Client (who are natural persons) ● Employees or contact persons of Client's prospects, Clients, business partners and vendors ● Employees, agents, advisors, freelancers of Client (who are natural persons) ● Client's users authorized by Client to use the Services
1.4 Nature and Purpose of Processing	Includes the following: The purpose of Processing of Client Personal Data by Planful is the performance of the Services pursuant to the Master Subscription Agreement.
1.5 Types of Personal Information	Includes the following: ● a name and surname; ● a home address; ● an email address such as name.surname@company.com; ● an identification card number; ● location data (for example the location data function on a mobile phone); ● an Internet Protocol (IP) address; ● a cookie ID; ● data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Exhibit B

EU Standard Contractual Clauses

1. **Incorporation of the EU SCCs.** For any transfer of Client Personal Data that is subject to the EU GDPR from the European Economic Area to a country outside the European Economic Area that is not the subject of an adequacy decision of the European Commission, the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the **"EU SCCs"**) are incorporated into this DPA by reference and form part of it, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. The Parties agree to be bound by the EU SCCs as completed by the module elections, optional-clause selections, and Annexes set out in this Exhibit B. Each Party is deemed to have signed the EU SCCs as of the Effective Date. To the extent of any conflict between the EU SCCs and any other term of this DPA or the Agreement, the EU SCCs prevail with respect to the subject matter they govern.

2. **Application and Modules.** Where applicable the EU SCCs apply as follows, and only the Module(s) corresponding to the applicable Processing scenario shall apply:

   (a) **Module Two (Controller to Processor)** applies where Client acts as a Controller of Client Personal Data and Planful Processes that Client Personal Data as a Processor on Client's behalf.

   (b) **Module Three (Processor to Processor)** applies where Client acts as a Processor on behalf of a third-party Controller and Planful Processes the relevant Client Personal Data as a sub-processor.

   (c) **Module One (Controller to Controller)** applies solely with respect to Planful Account Data and Planful Usage Data, for which Planful acts as an independent Controller pursuant to Section 3(l).

3. **Optional Clauses and Elections.** For each applicable Module, the following elections apply:

   (a) **Clause 7 (Docking clause):** does not apply.

   (b) **Clause 9 (Use of sub-processors) [Modules Two and Three]:** Option 2 (general written authorization) applies. Planful shall inform Client of any intended addition or replacement of sub-processors at least ten (10) days in advance, in the manner set out in Section 3(d), so as to give Client the opportunity to object before the sub-processor Processes Client Personal Data.

   (c) **Clause 11 (Redress):** the optional language providing for an independent dispute-resolution body does not apply.

   (d) **Clause 13 and Annex I.C (Supervision):** the competent supervisory authority is the Irish Data Protection Commission, as set out in Annex I.C.

   (e) **Clause 17 (Governing law):** Option 1 applies; the EU SCCs are governed by the law of Ireland.

   (f) **Clause 18(b) (Choice of forum):** any dispute arising from the EU SCCs shall be resolved before the courts of Ireland.

   (g) **Clause 8.9 / audits:** the data importer's audit obligations under the EU SCCs shall be satisfied in the manner, and subject to the limitations, set out in Section 8 (Audits) of this DPA.

Annex I

A. List of the Parties

Data Exporter

Name	As set forth in the Order Form
Address	As set forth in the Order Form
Contact	As set forth in the Order Form
Role	Controller (Modules One and Two); Processor (Module Three)
Activities relevant to the transfer	Receipt and use of the Services under the Agreement, including submission of Client Personal Data to the Services.
Signature and date	As set out in the DPA / Agreement; each Party is deemed to have signed the EU SCCs on the Effective Date.

Data Importer

Name	Planful, Inc.
Address	150 Spear Street, Suite 1700, San Francisco, CA 94105, USA
Contact	Data Protection Officer — dpo@planful.com
Role	Processor (Modules Two and Three); Controller (Module One)
Activities relevant to the transfer	Provision of the cloud-based financial planning and analysis Services under the Agreement.
Signature and date	As set out in the DPA / Agreement; each Party is deemed to have signed the EU SCCs on the Effective Date.

B. Description of the Transfer

- **Categories of data subjects:** as set out in Exhibit A, Section 1.3 (prospects, clients, business partners and vendors of Client who are natural persons; employees and contact persons of the foregoing; employees, agents, advisors and freelancers of Client who are natural persons; and Client's authorized users of the Services).
- **Categories of personal data:** as set out in Exhibit A, Section 1.5 (name and surname; postal address; email address; identification or card number; location data; Internet Protocol (IP) address; and cookie ID).
- **Sensitive data:** none. Client shall not submit special categories of personal data (as defined in Article 9 GDPR) to the Services, and the Services are not intended for the Processing of such data.
- **Frequency of the transfer:** on a continuous basis for the duration of the Agreement.
- **Nature and purpose of the Processing:** provision of the Services under the Agreement, as described in Exhibit A, Sections 1.1 and 1.4.
- **Period of retention:** for the term of the Agreement and, thereafter, for the return-or-deletion period specified in the Data Deletion provisions of this DPA.
- **Sub-processor transfers (Module Three):** for transfers to (sub-)processors, the subject matter, nature and duration of Processing are as described above and as further specified in Annex III / Exhibit C.

C. Competent Supervisory Authority

Consistent with Clause 13 and the governing-law election in this Exhibit B, the competent supervisory authority is the Irish Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland (with a further office at Canal House, Station Road, Portarlington, Co. Laois, R32 AP23, Ireland).

Annex II

Technical and Organisational Measures

The data importer maintains and enforces industry-standard technical and organisational measures designed to protect Client Personal Data against accidental or unlawful destruction, accidental loss, alteration, and unauthorized disclosure or access, and to ensure a level of security appropriate to the risk, consistent with Article 32 GDPR and the data importer's obligations under this DPA and the Agreement. These measures are described in the data importer's Information Security Addendum, available at https://planful.com/planful-information-security-addendum/and are further evidenced in the data importer's most recent SOC 2 Type II report, which is available to the data exporter upon written request, subject to reasonable confidentiality requirements. Such measures include, at a minimum:

- **Organisational control —** measures addressing internal organisation, including employee confidentiality commitments, data backup and deletion procedures, and logical separation of each customer's data.
- **Physical / entry control —** measures limiting physical access to facilities where Client Personal Data is Processed, including access controls at hosting facilities operated by the data importer's sub-processors.
- **System / admission control —** measures limiting access to systems on which Client Personal Data is Processed, including network safeguards and firewalls.
- **Access control —** least-privilege and role-based access, encryption, audit logging, individual user identifiers, strong authentication, and defined procedures for granting, changing, and revoking access rights.
- **Transmission control —** encryption of Client Personal Data in transit and at rest, and audit logging of data access.
- **Availability control —** failover capability, regularly tested backups stored in multiple locations, a disaster-recovery plan, and change management.
- **Separation control —** logical and, where appropriate, physical separation of data collected for different purposes and of different customers' data.

Assistance to the data exporter (Modules Two and Three): the data importer shall assist the data exporter in ensuring compliance with its obligations under Articles 32 to 36 GDPR, taking into account the nature of the Processing and the information available to the data importer, in the manner and subject to the cost-allocation set out in Sections 3(g) and 3(h) of this DPA.

Annex III

List of Sub-Processors

For Modules Two and Three, Client has authorized the engagement of the sub-processors identified in **Exhibit C** to this DPA and at https://planful.com/sub-processors/, as such list may be updated in accordance with Section 3(d) (Clause 9, Option 2). Each sub-processor is engaged under a written agreement imposing data-protection obligations substantially similar to those set out in this DPA, as required by Clause 9(c) of the EU SCCs.

planful

Exhibit C

Processing Locations

Planful's Primary Data Processing Locations

Facility	Location	Role
Primary Data Center – US	Digital Realty, Santa Clara, CA, USA	Third-party data center hosting FP&A Production application servers that store, process, and transmit data covered under this assessment.
Secondary (DR) Data Center – US	AWS, Northern Virginia, USA	Third-party cloud hosting FP&A Production (Secondary / Disaster Recovery) application servers for covered data.
Primary Data Center – Australia	Azure, Sydney, Australia	Third-party cloud hosting FP&A Production application servers for covered data.
Secondary (DR) Data Center – Australia	Azure, Melbourne, Australia	Third-party cloud hosting FP&A Production (Secondary / Disaster Recovery) application servers for covered data.
Primary Data Center – EU/UK	AWS, London, UK	Third-party cloud hosting FP&A Production application servers for covered data.
Secondary (DR) Data Center – EU/UK	AWS, Dublin, Ireland	Third-party cloud hosting FP&A Production (Secondary / Disaster Recovery) application servers for covered data.
Primary Data Center – Canada	AWS, Ontario (ON), Canada	Third-party cloud hosting FP&A Production application servers for covered data.
Secondary (DR) Data Center – Canada	AWS, Alberta (AB), Canada	Third-party cloud hosting FP&A Production (Secondary / Disaster Recovery) application servers for covered data.
Primary Data Center – EU (Marketing)	AWS, Frankfurt, Germany	Third-party cloud hosting the Planful for Marketing application for covered data.
Secondary (DR) Data Center – EU (Marketing)	AWS, Dublin, Ireland	Third-party cloud hosting Planful for Marketing (Secondary / Disaster Recovery) for covered data.
Primary Data Center – US (Marketing)	AWS, Northern Virginia, USA	Third-party cloud hosting the Planful for Marketing application for covered data.
Secondary (DR) Data Center – US (Marketing)	AWS, US West Coast, USA	Third-party cloud hosting Planful for Marketing (Secondary / Disaster Recovery) for covered data.
Non-production Data Center – US	AWS, Oregon, USA	Third-party cloud hosting Planful non-production environments (staging, sandbox, sustenance, etc.).

Network Operations Center (NOC) – US	San Francisco, CA, USA	Remote production support and back-office work. No covered production data stored at this location.
Network Operations Center (NOC) – India	Hyderabad, India	Remote production support and back-office work. No covered production data stored at this location.
Corporate Office – US	San Francisco, CA, USA	Corporate office: Trust–Compliance–Security, Customer Support, HR, Sales & Marketing, Executive Management.
Application Development Center (R&D / Engineering)	Hyderabad, India	Overseas office: Engineering, QA, Security Testing, Customer Support, HR.
Regional Office	London, UK	Sales Development.
Regional Office	Toronto, Canada	Sales Development.

Sub-Processors

Company Name	**Sub-processing Activities**	**Location**	**Country**
AWS Inc. (US, Canada, UK, Ireland)	Hosting of Financial Planning Services	Northern Virginia Oregon Calgary Toronto London Dublin Sydney	United States United States Canada Canada United Kingdom Ireland Australia

AWS Inc. (US, Canada, EU)	Hosting of Marketing Planning Services	Northern Virginia Oregon Calgary Toronto Dublin Frankfurt	United States United States Canada Canada Ireland Germany
Microsoft Azure	Hosting of Financial Planning Services	Sydney Melbourne	Australia Australia
Digital Realty	Hosting (US Data only) of Financial Planning Services	Northern California	United States
Pendo.io Inc.	In product communications and survey for Financial Planning Services	San Francisco, CA /Hyderabad	United States, India
NetSuite	Data Management (only applicable when Client purchases the integration)	San Francisco, CA /Hyderabad	United States, India
Salesforce	Support Ticketing	San Francisco, CA /Hyderabad	United States, India
Gainsight	Product Usage Analytics and in product engagement	San Francisco, CA /Hyderabad	United States, India
Trend Micro	Cloud Security for Marketing Planning Services	Northern Virginia Oregon Dublin Frankfurt	United States United States Ireland Germany

Boomi* *Boomi is only a sub-processor for Clients who purchased Boomi connectors with their Planful subscription	Data Integration Services for Financial Planning Services	Northern California Northern Virginia London Dublin Sydney Melbourne	United States United States United Kingdom Ireland Australia Australia
OpenAI L.L.C.	Machine Learning/AI Data Processing for Financial Planning Services (only applies	San Francisco, CA /Hyderabad	United States, India
OpenAI L.L.C.	Machine Learning/AI Data Processing for Financial Planning Services (only applies	San Francisco, CA /Hyderabad	United States, India

Exhibit D
International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

The Parties agree that to the extent there are transfers of Personal Data from the United Kingdom, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, issued by the UK ICO under S119A(1) Data Protection Act 2018 and in force March 21, 2022 (the "UK SCCs"), are hereby incorporated by reference and apply to this DPA.

In addition, where the UK SCCs identify optional provisions (or provisions with multiple options) the following shall apply:

Part 1 Tables:

Table 1: The party details and contact information in Table 1 of the UK SCCs shall be the party details and contact information as set out in Annex 1 of the EU SCCs. The start date shall be the effective date of the DPA.

Table 2: Exhibit B to the DPA sets out the version of the Approved EU SCCs which this Addendum is appended to, including the selected modules, clauses, optional provisions and Appendix Information.

Table 3: "Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in Exhibit B to the DPA:
-Annex 1 (Description of Transfer; the list of Parties)
-Annex 2 (Technical and Organisational Measures)
-Annex 3 attached hereto as Exhibit C (List of Sub processors, if any).

Part 2 Mandatory Clauses: Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses, are incorporated by reference.

Exhibit E
Swiss Standard Contractual Clauses Addendum

The Parties agree that for transfers of Personal Data from the Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), the terms of the EU SCCs shall be amended and supplemented as specified by the relevant guidance of the Swiss Federal Data Protection and Information Commissioner, and the following provisions shall apply:

1. General and specific references in the EU SCCs to GDPR, or EU or Member State Law, shall have the same meaning as the equivalent reference in Swiss Data Protection Laws.

2. In respect of data transfers governed by Swiss Data Protection Laws, the EU SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

3. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

4. In respect of disputes, the choice of forum and jurisdiction as set out in the EU SCCs shall apply. For Data Subjects habitually resident in Switzerland, the law and courts of Switzerland are an alternative place of jurisdiction