



## DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**Addendum**”) forms part of the Master Subscription Agreement (the “**Agreement**”) between PLANFUL, INC. (“**Planful**”) and (“**Company**”) (collectively the “**Parties**”).

### 1. Subject Matter and Duration.

- a) **Subject Matter.** This Addendum reflects the Parties’ commitment to abide by Applicable Data Protection Laws 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 Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.
- b) **Duration and Survival.** This Addendum will become legally binding upon the Effective Date of the Agreement or upon the date that the Parties sign this Addendum 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 Addendum will continue in effect so long as Planful Processes Client Personal Data.

### 2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

- a) “**Applicable Data Protection Law(s)**” means the relevant data protection and data privacy laws, rules and regulations to which the Client Personal Data are subject. “Applicable Data Protections Law(s)” shall include, but not be limited to, the EU General Data Protection Regulation 2016/679 (“**GDPR**”) and California Consumer Privacy Act (“**CCPA**”).
- b) “**Client Personal Data**” means Personal Data Processed by Planful pertaining to Client’s business and related to individuals located in the European Economic Area and California. 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) “**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.
- f) “**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 Addendum.
- g) “**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.



- h) **“Services”** means any and all services that Planful performs under the Agreement, including Application Services.
- i) **“Swiss Addendum”** means the Swiss Standard Contractual Clauses Addendum as set out in Exhibit E of this Addendum.
- j) **“Third Party(ies)”** means Planful’s authorized contractors, agents, vendors and third party service providers (i.e., sub-processors) that Process Client Personal Data.
- k) **“UK Addendum”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses set out in Exhibit D of this Addendum.

### 3. Data Use and Processing.

- a) **Compliance with Laws.** Client Personal Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).
- b) **Documented Instructions.** 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 Addendum, 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.
- c) **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 will 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. Parties agree to work in good faith on resolving any objections to the use of sub-processors by Planful.
- d) **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.
- e) **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.
- f) **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 Personal Data granted to them under Applicable Data Protection Law(s) (**“Privacy Request”**). At Client’s request and without undue delay, Planful will use commercially reasonable measure to assist Client in answering or complying with any Privacy Request in so far as it is possible.



- g) 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.
- h) 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.

#### 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.

#### 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) (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 the 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;
  - 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.

#### 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 of Security Incidents, document Security Incidents and their outcomes, and (ii) 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 available details required under Applicable Data Protection Law(s) for Client



to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

**7. 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 28 days after such termination or expiration, Planful will provide Client with temporary access to the Planful platform to retrieve any Client or transaction log data left in Planful’s system.

**8. 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: \_\_\_\_\_

<p><b>[CLIENT],</b> a(n) _____</p> <p>Signature: _____</p> <p>Printed Name: _____</p> <p>Title: _____</p>	<p><b>Planful, Inc.,</b> a(n) Delaware Corporation _____</p> <p><small>DocuSigned by:</small></p> <p>Signature: <u>Eugenia Bergantz</u></p> <p>Printed Name: <u>Eugenia Bergantz</u></p> <p>Title: <u>General Counsel</u></p>
---	---



### Exhibit A

1.1 Subject Matter of Processing	<p>The Processing will involve Processing for data and application integration services.</p> <p>The subject matter of Processing is the Services pursuant to the Master Subscription Agreement.</p>
1.2 Duration of Processing	<p>The Processing will continue until the expiration or termination of the Master Subscription Agreement.</p>
1.3 Categories of Data Subjects	<p>Includes the following:</p> <ul style="list-style-type: none"> <li>● Prospects, Clients, business partners and vendors of Client (who are natural persons)</li> <li>● Employees or contact persons of Client's prospects, Clients, business partners and vendors</li> <li>● Employees, agents, advisors, freelancers of Client (who are natural persons)</li> <li>● Client's users authorized by Client to use the Services</li> </ul>
1.4 Nature and Purpose of Processing	<p>Includes the following:</p> <p>The purpose of Processing of Client Personal Data by Planful is the performance of the Services pursuant to the Master Subscription Agreement.</p>
1.5 Types of Personal Information	<p>Includes the following:</p> <ul style="list-style-type: none"> <li>● a name and surname;</li> <li>● a home address;</li> <li>● an email address such as <a href="mailto:name.surname@company.com">name.surname@company.com</a>;</li> <li>● an identification card number;</li> <li>● location data (for example the location data function on a mobile phone);</li> <li>● an Internet Protocol (IP) address;</li> <li>● a cookie ID;</li> <li>● data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.</li> </ul>



**Exhibit B**

**Standard Contractual Clauses (Processors)**

For the purposes of Article 28(3) and (4) and Chapter 5 of the EU General Data Protection Regulation 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation:

Address:

Tel.: \_\_\_\_\_; fax: \_\_\_\_\_; e-mail: \_\_\_\_\_

Other information needed to identify the organisation

.....  
(the data **exporter**)

And

*[The gaps below are populated with details of the relevant Contracted Processor:]*

Name of the data importing organisation: Planful, Inc.

Address: 150 Spear Street, Suite 1850, San Francisco, CA 94105

Tel.: \_\_\_\_\_; fax: \_\_\_\_\_; e-mail: legal@Planful.com

Other information needed to identify the organisation:

.....  
(the data **importer**)  
each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.



## STANDARD CONTRACTUAL CLAUSES

1. The Standard Contractual Clauses (“SCCs”) found at [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en), or any successor website or we address designated by the EU Commission shall apply to the transfer of European Union Personal Data outside of the European Union.
2. The following shall apply to the SCCs, including the election of specific terms or optional clauses as described in more detail below, and any options clauses not expressly selected are not included below.
  - a) In relation to Personal Data that is protected by the GDPR, the EU SCCs will apply as follows:
    - i) Planful will be the “Data Importer” and Client will be the “Data Exporter”;
    - ii) The terms of Module 2, “Transfer Controller to Processor,” shall apply;
    - iii) In Clause 7, the optional docking clause shall not apply;
    - iv) In Clause 9, Option 2 shall apply and the period for prior notice of Sub-Processor changes shall be contingent on Client opting into notifications regarding such additions at <https://planful.com/sub-processors/>. Once opted in, Planful shall notify Client of any proposed amendments to the Sub-Processor List (including the addition or any replacement to the list) at least ten days prior to any such change;
    - v) In Clause 11, the optional language shall not apply;
    - vi) In Clause 17, Option 1 shall apply, and the EU SCCs shall be governed by Irish Law;
    - vii) In Clause 18(b) disputes shall be resolved before the Courts of Ireland;



**ANNEX I**

**A. LIST OF PARTIES**

Data exporter(s): Client.

Name:

Address:

Contact person’s name, position and contact details:

Activities relevant to the data transferred under these Clauses:

\_\_\_\_\_  
\_\_\_\_\_

Signature: \_\_\_\_\_

Role (controller/processor):

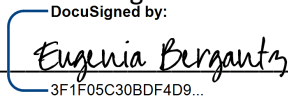
Data importer(s): Planful is the leading provider of cloud-based enterprise performance management (EPM) software solutions. Planful enterprise performance platform helps finance departments and executives improve their modeling, planning, consolidation, reporting, and analytics processes.

Name: Planful Inc.

Address: 150 Spear Street Suite 1850 San Francisco, CA 94105

Contact person’s name, position and contact details: Eugenia Bergantz, General Counsel, legal@planful.com

Activities relevant to the data transferred under these Clauses: The personal data transferred will be processed in performance of the provision of services by data importer to data exporter in accordance with the terms of all agreements between the parties, including these Clauses.

Signature:  \_\_\_\_\_  
3F1F05C30BDF4D9...

Role (controller/processor):

**B. DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

The personal data transferred may concern data exporter’s and its Affiliates’ clients’ and prospective clients’ representatives and end users, as well as employees of data exporter and its Affiliates.

Categories of personal data transferred





The personal data transferred may include the following information regarding the data subjects: legal names, partial names and nicknames; titles; positions; employer; salary history; work contact information (including work email addresses), country of residence, nationality and connection and localisation data (including IP addresses, cookie ID).

Planful does not knowingly collect (and Client shall not knowingly submit) any special categories of data (as defined under the Data Protection Laws) and terms of this addendum or contract does not permit customers or end users of the EPM cloud services to upload any such special categories of data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

The personal data transferred will be processed in performance of the provision of services by data importer to data exporter in accordance with the terms of all agreements between the parties, including these Clauses.

Purpose(s) of the data transfer and further processing

Enforcement of contract and fulfillment of contractual obligations

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data shall be retained for the duration of the contract and up to 28 days after termination while Planful fulfills its post-termination obligations to Client in accordance with the MSA and DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The sub-processors listed in Exhibit C will receive data to fulfill Planful's contractual obligations to Client and improve the Application Services for the duration of the contract or as otherwise required by law.

## **C. COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority is the Office of the Data Protection Commissioner located at Canal House, Station Road, Portarlinton, Co. Laois, R32 AP23, Ireland.



## ANNEX II

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data Importer maintains and enforces industry standard technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and ensure a level of security appropriate to the risk of its processing of Personal Data processing consistent with its obligations under the Agreement and the GDPR. These measures shall include a comprehensive information security program that includes administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data that are appropriate to the type of information that Data Importer will process. Data Importer shall regularly monitor compliance with these safeguards.

Core technical and organizational security measures implemented by Data Importer as of the date of signature are described in Data Importer's most current SOC audit reports, which will be provided to Data Exporter upon request.

To mitigate the risk to information processing resources, unauthorized disclosure or erasure of information and interruption of support for business processes which may result from unauthorized access, security controls implemented by the Data Importer are included in the following sections:

- Organizational Control – Measures which comply with the specific requests of Data Protection, regarding the internal organization such as commitment of employees to data secrecy, data backup/deletion, spatial/personal separation of data from other Clients etc.
- Entry Control – Measures to limit entrance of unauthorized persons to areas where personal data is used or processed such as gate control, identification badges/code cards etc.
- Admission Control – Measures to limit admission of unauthorized persons to systems where personal data is used or processed such as safeguarding of physical network infrastructure, firewalls etc.
- Access Control – Measures to limit access of unauthorized persons to systems where personal data is used or processed such as having least privilege/selective access policy, use of encryption, audit logging, individual user ids/strong passwords, regulated procedures for granting, changing and revocation of access rights etc.
- Transmission Control – Measures to ensure that personal data cannot be read, copied, modified or removed without authorization such as use of encryption both at rest and in transit, audit logging to have retrospect information which data has been retrieved by whom etc.
- Availability Control – Measures to ensure that personal data is protected from accidental destruction or loss such as fail over capabilities, regular tested backups stored in multiple locations and disaster recovery plan, change management process etc.



- Separation Control – Measures to ensure that data collected for different purposes can be processed separately such use of separate user roles, logical/physical separation of data etc.



**Exhibit C**

**List of Sub-Processors**

<b>Company Name</b>	<b>Sub-processing Activities</b>	<b>Location</b>	<b>Country</b>
AWS Inc. (UK, Ireland)	Hosting of Financial Planning Services	Northern Virginia	United States
		Oregon	United States
		London	United Kingdom
		Dublin	Ireland
		Sydney	Australia
AWS Inc. (US, EU)	Hosting of Marketing Planning Services	Northern Virginia	United States
		Frankfurt	Germany
Microsoft Azure	Hosting of Financial Planning Services	Melbourne	Australia
Digital Realty	Hosting (US Data only) of Financial Planning Services	Northern California	United States
Waverley Software	Software development services	Europe	Ukraine
			Poland
			Austria
			Spain



Pendo.io Inc.	In product communications and survey for Financial Planning Services	Redwood City, CA /Hyderabad	US, India
NetSuite	Data Management (only applicable when Client purchases the integration)	Redwood City, CA /Hyderabad	US, India
Salesforce	Support Ticketing	Redwood City, CA /Hyderabad	US, India
HubSpot	CRM Cloud Services for Marketing Planning Services	Northern Virginia	US
Gainsight	Product Usage Analytics and in product engagement	Redwood City CA /Hyderabad	US, India
ChurnZero	Customer Success Management for Marketing Planning Services	Northern Virginia	US
Trend Micro	Cloud Security for Marketing Planning Services	Northern Virginia	US



**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.