

OnePlan Portfolio Solutions Data Processing Agreement

Where applicable, this Data Processing Agreement is hereby incorporated in the OnePlan Terms of Use (the "**Terms**"), found at <https://oneplan.ai/terms>, unless the Customer has entered into a superseding written agreement with OnePlan Portfolio Solutions, LLC or its subsidiaries including OnePlan Portfolio Solutions Canada, in which case, it forms a part of such written agreement. All capitalized terms not defined herein shall have the meaning set forth in the Terms.

WHEREAS

- A. The Customer acts as a Data Controller.
- B. The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor (OnePlan Portfolio Solutions).
- C. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- D. The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS

1. Definitions and Interpretation

- 1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
 - 1.1.1. "**Agreement**" means this Data Processing Agreement and all Schedules;
 - 1.1.2. "**Customer Personal Data**" means any Personal Data Processed by Processor or a Subprocessor on behalf of the Customer pursuant to or in connection with the Principal Agreement;
 - 1.1.3. "**Data Controller**" means the entity that determines the purposes and essential means of processing Personal Data.
 - 1.1.4. "**Data Processor**" means the entity that processes Personal Data on behalf of, and in accordance with the instructions of, the Data Controller.
 - 1.1.5. "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country, as applicable;
 - 1.1.6. "**Data Transfer**" means:
 - 1.1.6.1. a transfer of Customer Personal Data from the Customer to a Subprocessor ; or
 - 1.1.6.2. an onward transfer of Customer Personal Data from a Subprocessor to a Subcontracted Processor, or between two establishments of a Subprocessor.

In each case, where such transfer would be prohibited by Data

Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

- 1.1.7. **"EEA"** means the European Economic Area;
- 1.1.8. **"EU Data Protection Laws"** means the General Data Protection Regulation (EU) 2016/679 ("GDPR") and any applicable implementing or supplementary legislation in EU Member States or the EEA. ;
- 1.1.9. **"GDPR"** means EU General Data Protection Regulation 2016/679;
- 1.1.10. **"Services"** means the SaaS services the Data Processor provides;
- 1.1.11. **"Subprocessor"** means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Customer in connection with the Agreement:
 - 1.1.11.1. The Customer hereby approves those third parties listed below (the "Subprocessors"), which are compliant with GDPR requirements regarding transfers of Customer Personal Information to a third country:
 - Microsoft Azure. OnePlan's solutions are hosted in Microsoft Azure data centers.
 - Zendesk. OnePlan's customer service tool is Zendesk.

1.2. The terms, **"Commission"**, **"Controller"**, **"Data Subject"**, **"Member State"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"** and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Customer Personal Data

- 2.1. Processor acts solely as a processor and does not act as a joint controller with Customer.
- 2.2. In Processing Customer Personal Data, Processor agrees that:
 - 2.2.1. Subject to Section 2.3 below, Processor shall process Customer Personal Data only on documented instructions from Customer;
 - 2.2.2. Processor's personnel are under confidentiality obligations;
 - 2.2.3. Processor has implemented security measures meeting Article 32 GDPR;
 - 2.2.4. Subprocessors are subject to the same obligations;
 - 2.2.5. Processor shall assist Customer with data subject requests;
 - 2.2.6. Processor shall assist Customer with security, breach notifications, DPIAs, and consultations;
 - 2.2.7. Upon termination, Processor shall delete or return data in accordance with Section 9 of this Agreement.
 - 2.2.8. Processor shall make available information necessary to demonstrate compliance and allow audit.
- 2.3. Processor shall comply with all other applicable Data Protection Laws in the Processing of Customer Personal Data as currently enacted, or as may be enacted, or as revised from time-to-time during the term of this Agreement.

- 2.4. Processor shall process Customer Personal Data only on documented instructions from Customer, unless processing is required by applicable law. Processor shall notify Customer before processing under such law unless prohibited.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Subprocessor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Subprocessor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

- 4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
- 4.2. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

- 5.1. Customer provides general authorization for Processor to engage Subprocessors as reasonably necessary to provide the Services.
- 5.2. Processor shall maintain a current list of all current Subprocessors, which shall be made available at <https://trust.oneplan.ai/subprocessors>, and shall notify Customer of any material changes.
- 5.3. Customer may object on reasonable data protection grounds; Processor may (a) propose alternatives, (b) mitigate the concern, or (c) allow termination of the affected Services.
- 5.4. Processor shall not appoint (or disclose any Customer Personal Data to) any Subprocessor unless required to provide its services, or as otherwise authorized by Customer.

6. Data Subject Rights

- 6.1. Taking into account the nature of the Processing, Processor shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by the Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 6.2. Processor shall:
 - 6.2.1. promptly notify the Customer if it receives a request from a Data Subject under any Data Protection Law in respect of the Customer's Personal Data; and
 - 6.2.2. ensure that it does not respond to that request except on the documented instructions of the Customer or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the Subprocessor responds to the request.

7. Personal Data Breach

- 7.1. Processor shall notify the Customer without undue delay upon Processor becoming aware of a Personal Data Breach affecting the Customer's Personal Data, providing the Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 7.2. Processor shall co-operate with the Customer and take reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Not more than once per calendar quarter, upon the reasonable request of Customer, Processor shall provide reasonable assistance to Customer with any data protection impact assessments on systems storing Customer's data, and consultations with Supervising Authorities or other competent data privacy authorities, which the Customer reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of the Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Subprocessor.

9. Deletion or return of Customer Personal Data

- 9.1. Upon written request or cessation of the Services, Processor shall delete or return active copies of Customer Personal Data within thirty (30) days, unless a longer period is required by applicable law.
- 9.2. Customer acknowledges that Customer Personal Data may retain in secure system backups, archives and logs, which are deleted on standard rotation schedules
- 9.3. Processor shall certify deletion of active data upon request, but it is not required to delete or modify historical backups prior to their scheduled expiration.

10. Audit rights

- 10.1. Subject to this Section 10, Upon Customer's reasonable request, but in any event, not at a greater frequency than once per calendar quarter, Processor shall make available to the Customer all information necessary to demonstrate Supplier's compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer's Personal Data by the Subprocessors, provided that Customer's requests are reasonable, are conducted not more than once per calendar quarter during Processor's normal business hours and conducted in a fashion to be as least disruptive to Processor's operation as possible.
- 10.2. Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

- 11.1. Customer may choose a hosting region from those offered by Processor, including the EU (eu.oneplan.ai, Azure Netherlands).
- 11.2. Customer authorizes Processor to transfer Customer Personal Data outside the EEA as needed to provide the Services, including support and operations performed from the United States and Canada, provided such transfers comply with applicable Data Protection Laws.

- 11.3. Processor uses the EU Standard Contractual Clauses, the EU-U.S. Data Privacy Framework (where applicable), or other lawful mechanisms for such transfers.
- 11.4. Processor shall ensure an equivalent level of protection as required by applicable laws.

12. Governing Law and Jurisdiction

- 12.1. This Agreement is governed by the laws of the state of California, United States. Notwithstanding the foregoing, for data transfers governed by the Standard Contractual Clauses (“**SCCs**”), the SCCs’ choice of law and jurisdiction shall apply.
- 12.2. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of California, subject to possible appeal to the United States Federal Court.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

OnePlan Portfolio Solutions, LLC

[Customer]

B y : By: _____
 _____ [name]
 [name] [title]
 [title]

D a t e : Date: _____

SCHEDULE 1
DATA PROCESSING DETAILS

Subject Matter	The provision of OnePlan SaaS services.
Duration:	Term of Agreement + retention period.
Nature & Purpose:	Hosting, storage, display, analysis, authentication, dashboards, reporting, optional AI features, and support.
Categories of Personal Data:	Name, email, role/department, identifiers, metadata, customer-entered optional fields.
Data Subjects:	Customer employees and contractors.
Processing Activities:	Storage, retrieval, display, modification, transmission, support access, deletion.
Subprocessors:	Listed at https://trust.oneplan.ai/subprocessors
International Transfers:	Governed by Section 11 and applicable SCCs.