Data Processing Agreement

1. SCOPE

1.1. These Data Processing Terms (hereinafter referred to as "DPA") shall apply to the provision of Platform and Services by AppXite, as well as theprocessing of data under the AppXite Platform and Service Agreement.

2. DEFINITIONS AND INTERPRETATIONS

2.1. For the purposes of the DPA the following terms shall have the meaning ascribed to them as follows:

"***Applicable Data Protection Law***" means European Union General Data Protection Regulation (hereinafter referred to as "GDPR") or other EU legislation that may be promulgated from time to time, any national or internationally binding data protection laws or regulations applicable at any time during the term of this DPA on, as the case may be, the Controller or the Processor. "***Applicable Data protection laws***" includes any binding guidance, opinions or decisions of regulatory bodies, courts or other bodies, as applicable;	"***Process or Processing***" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"***Personal Data***" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;	"***Processor***" means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person;
"**Platform**" means the cloud commerce platform software as a service owned by AppXite and provided to partner as a white label solution. Platform is designed to manage sales and business operations and enables Partner to market Products to various re-sellers or customers;	"**Services**" means services provided by AppXite, including but not limited to, CSP Support Services, white label billing and other services AppXite makes available for purchase from time to time;
"***Agreement***" means the agreement with AppXite for the provision of platform or Services or AppXite Partner Program (e,g, Reseller Agreement; Sales Solution Agreement);	"***Pseudonymisation***" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
"***Controller***" means the party hereto as stated above which alone or jointly with others, determines the purposes and means of the processing of Personal Data;	"***Supervisory Authority***" means an independent public authority which is established pursuant to GDPR Article 51;

"***Partner***" means the contracting party of AppXite under the relevant Agreement;	"***Data Subject***" means an identified or identifiable natural person;
"***Personal Data Breach***" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;	"***Sub-processor***" means a third-party subcontractor engaged by the Processor which, as part of the subcontractor's role of delivering the services, will Process Personal Data on behalf of the Controller;

3. ROLES AND RESPONSIBILITIES

3.1. Partner and AppXite hereby agree that in the context of this DPA, the Partner is a Controller of Personal Data and the AppXite is a Processor of Personal Data. Notwithstanding the foregoing, in some cases defined herein AppXite may be regarded as Controller; or Sub-Processor (whereas Partner acts as a Processor).

4. PROCESSING DETAILS

Purposes of processing	The purposes of the processing are the delivery of the following services or tasks by the Processor to the Controller; ☒ AppXite Platform; ☒ Authentication; ☒ Reseller Authorization in accordance with the AppXite Reseller Terms; ☐ White Label Billing; ☐ IT Support; ☐ Managed Services.
Categories of data	First Name, Last Name, email address, phone number.
Categories of data subjects	Customers End Users Contractors Employees
Processing operations/activities	Processing operations may include: collection, access, organization, structuring, storage, retrieval, consultation, use, restriction, erasure or destruction.
Location of processing operations include	EEA, USA.
Sub-Processors	Microsoft Corporation, Auth0.
Duration of Processing/ Term of this DPA	This DPA is valid for the term of the agreement between AppXite and Partner and until all Personal Data is deleted or returned in accordance with Partner instructions (unless provided otherwise in the agreement between parties hereto).

5. PROCESSING OF PERSONAL DATA

5.1. The Processor guarantees that it has implemented and will continue to implement within the term of this DPA the appropriate technical and organizational measures in such a manner that its Processing of Personal Data under this DPA will meet the requirements of Applicable Data Protection Law and ensure the protection of the rights of the Data Subject.

5.2. The Processor undertakes to only Process Personal Data in accordance with documented instructions communicated from time to time by the Controller, unless required to do so pursuant to the Applicable Data Protection Law. The Processor shall at any time be able to document the specific instructions from the Controller. The Controller guarantees that it is entitled to Process the Personal Data under Applicable Data Protection Law before providing Personal Data to the Processor. The Controller hereby confirms that it is solely responsible for determining the purposes and means of processing Personal Data by the Processor. The Controller's initial instructions to the Processor regarding the subject-matter and duration of the processing, the nature and purpose of the Processing, the type of Personal Data, and categories of data subjects are set forth in the Section 4. of the DPA.

5.3. The Processor shall, when processing Personal Data under this DPA, comply with Applicable Data Protection Law and applicable recommendations by the Supervisory Authority or other competent authorities. The Processor shall accept to make any changes and amendments to this DPA that are required under Applicable Data Protection Law.

5.4. The Processor shall assist the Controller in fulfilling its legal obligations under Applicable Data Protection Law, including, but not limited to, the Controller's obligation to respond to requests for exercising the Data Subject's rights to request information (register extracts) and for Personal Data to be corrected, blocked or erased.

5.5. The Processor shall immediately inform the Controller if the Processor does not have an instruction for how to process Personal Data in a situation or if any instruction provided under this DPA or otherwise infringes Applicable Data Protection Law.

5.6. If Data Subjects, competent authorities or any other third parties request information from the Processor regarding the Processing of Personal Data covered by this DPA, the Processor shall refer such request to the Controller. The Processor may not in any way act on behalf of or as a representative of the Controller.

5.7. The Processor may not, without prior instructions from the Controller, transfer, or in any other way, disclose Personal Data or any other information relating to the Processing of Personal Data to any third party. In the event that the Processor, according to Applicable Data Protection Law, is required to disclose Personal Data that the Processor Processes on behalf of the Controller, the Processor shall be obliged to inform the Controller thereof immediately and request confidentiality in conjunction with the disclosure of requested information.

5.8. Upon the Controller's reasonable request, and in accordance with the change management procedure set forth in the respective Agreement (if applicable), the Processor shall implement additional reasonable technical and organizational security measures and adjustments to the processing activities. The Controller shall notify the Processor of any adjustments to the Controller's instructions concerning security and the processing of Personal Data, without undue delay, for the Processor to enable the necessary amendments to procedures to be implemented.

5.9. The Processor undertakes to make available to the Controller all information and provide all assistance necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including on-site inspections, conducted by the Controller or another auditor mandated by the Controller.

6. SUB PROCESSORS

6.1. The Controller agrees that companies listed in the Section 4 of this DPA may be retained as Sub-Processors under this DPA.

6.2. The Processor will inform the Controller of any intended changes concerning the addition or replacement of Sub Processors. All new Sub-processors will enter into data processing agreement that contains the mandatory requirements governed by Article 28 (3) of the GDPR, accept privacy terms and other rules associated with information security.

6.3. The Processor shall remain fully liable to the Controller for the performance of the Sub Processor's obligations.

7. TRANSFER TO THIRD COUNTRIES

7.1. Any transfer of Personal Data to a state which is not listed in the Section 4 of this DPA requires prior notification of the Controller (with the right to object) and compliance with the Chapter V of the GDPR, by signing Model Clauses for personal data transfer outside EU, to ensure that personal data protection requirements are applied contractually for the Controller/Processor outside EU and EEA.

8. INFORMATION SECURITY AND CONFIDENTIALITY

8.1. The AppXite can demonstrate its compliance with the obligations in this DPA by maintaining the ISO 27001 Information Security Management certification, therefore, having an independent auditor's note that AppXite's information security practices are in conformity with ISO 27001 requirements.

8.2. The Processor shall, in order to assist the Controller to fulfil its legal obligations including but not limited to; security measures and privacy impact assessments, be obliged to take appropriate technical and organizational measures to protect the Personal Data which is Processed and shall thereby follow any written information security requirements or policies communicated by the Controller from time to time. The measures shall at least result in a level of security which is appropriate taking into consideration:

i. the technical possibilities available;
ii. the cost to implement the measures;
iii. the special risks involved with processing of personal data; and
iv. the sensitivity of the personal data.

8.3. The Processor shall maintain adequate security for the Personal Data appropriate to the risk of processing.

8.4. The Processor shall protect the Personal Data against destruction, modification, unlawful dissemination, or unlawful access. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the technical and organizational measures to be implemented by the Processor shall include, inter alia, as appropriate:

i. the Pseudonymisation and encryption of Personal Data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing Personal Data;

iii. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.5. The Processor shall maintain a record of all categories of Processing activities carried out on behalf of the Controller. The Processor shall prepare and keep updated a description of its technical, organisational and physical measures to be and maintain compliant with the Applicable Data Protection Law.

8.6. The Processor undertakes not to, without the Controller's prior written consent disclose or otherwise make Personal Data Processed under this DPA available to any third party, except for Sub Processors engaged in accordance with this DPA.

8.7. The Processor shall be obliged to ensure that only persons that directly require access to Personal Data in order to fulfil the Processor's obligations in accordance with the respective Agreement have access to such information. The Processor shall ensure that any persons involved in the Processing of Personal Data have committed themselves to confidentiality or are under proper statutory obligation of confidentiality.

9. PERSONAL DATA BREACH

9.1. In case of a Personal Data Breach involving Personal Data Processed on behalf of the Controller the Processor shall, taking into account the nature of Processing and the information available to the Processor, assist the Controller in ensuring compliance with the Controllers obligations pursuant to article 33 in the GDPR. Further the Processor shall notify the Controller without undue delay, but not later than 24 hours after becoming aware of such a Personal Data Breach. The notification shall at least:

i. describe the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned, the categories and approximate number of Personal Data records concerned;

ii. communicate the name and contact details of the contact point where more information can be obtained;

iii. describe the likely consequences of the Personal Data Breach;

iv. describe the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.