Data Processing Agreement

1. INTRODUCTION

1.1. The parties agree that this Data Processing Agreement (hereinafter referred to as "***DPA***") sets forth their obligations with respect to the processing of Personal Data in connection with provision of Platform and Services. This DPA is incorporated by reference into the AppXite Partner Agreement. For the avoidance of doubt, this DPA shall not apply to any data processed Products purchased by the Partner through the Platform.

1.2. Please note that AppXite's security commitments and obligations outlined in this DPA shall not apply to the Trial/Sandbox Platform and Services.

1.3. Please note that AppXite may, from time to time, modify this DPA by publishing the most current version on the AppXite Legal Hub to New features, services, and components we add to the Platform are subject to this Agreement. By continuing to use the Platform or any service governed by this Agreement after the modification comes into effect, you are agreeing to be bound by the modified 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 performed in relation to Personal Data or 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;
- "***Agreement***" means the AppXite Partner Agreement for the provision of Platform or Services to Partner;
- "***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 agree that in the context of this DPA, the Partner is the Controller of Personal Data and AppXite is the Processor of Personal Data, except when the Partner acts as a Processor, in which case AppXite is a sub-processor. Whereas Partner is a processor, the Partner warrants to AppXite that Partner's processing related instructions to AppXite have been authorized by the relevant Controller.

3.2. Partner agrees that AppXite may process the Personal Data as Controller for the purposes of AppXite's internal operations. AppXite undertakes to safeguard such Personal Data and process it to the extent required for carrying out its internal operations outlined in the Annex I. AppXite acknowledges its accountability for such processing as Controller according to the Article 5 (2) of the GDPR.

4. OBLIGATIONS OF THE PARTIES

4.1. **Description of Processing**

(a) The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Partner, are specified in the Annex I.

4.2. **Instructions**

(a) The AppXite shall process Personal Data in only on documented instructions communicated from time to time by the Partner, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so according to the Applicable Data Protection Law. In this case, AppXite shall inform the Partner of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Partner throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) AppXite shall immediately inform the Partner if, in the AppXite's opinion, instructions given by the Partner infringe the Applicable Law.

(c) The Partner guarantees that it is entitled to Process the Personal Data under Applicable Data Protection Law before providing Personal Data to AppXite. Partner hereby confirms that it is solely responsible for determining the purposes and means of processing Personal Data by the AppXite.

4.3. **Purpose Limitation.**

(a) AppXite shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the Partner.

4.4. **Duration of the Processing of Personal Data**

(a) Processing by the AppXite shall only take place for the duration specified in Annex I.

4.5. **Security of Processing**

(a) AppXite shall at least implement the technical and organizational measures specified in the Security and Compliance Whitepaper to ensure the security of the Personal Data. This includes protecting the data against

a Personal Data Breach. The measures shall at least result in a level of security which is appropriate taking into consideration:

a. the technical possibilities available;

b. the cost to implement the measures;

c. the special risks involved with processing of personal data; and

d. the sensitivity of the personal data.

(b) The technical and organizational measures to be implemented by AppXite shall include, inter alia, as appropriate:

a. the Pseudonymization and encryption of Personal Data;

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

c. 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

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

(c) AppXite shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. AppXite shall be obliged to ensure that only persons that directly require access to Personal Data in order to fulfil the AppXite's obligations in accordance with the respective Agreement have access to such information. AppXite 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.

(d) AppXite undertakes not to, without the Partner'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.

(e) AppXite shall take all measures required pursuant to Article 32 of the GDPR.

(f) If the processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**Sensitive Data**"), AppXite shall apply specific restrictions and/or additional safeguards.

4.6. **Documentation and Compliance**

(a) The Parties shall be able to demonstrate compliance with this DPA.

(b) AppXite shall deal promptly and adequately with inquiries from the Partner about the processing of Personal Data in accordance with this DPA.

(c) AppXite shall make available to the Partner all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from the Applicable Law.

(d) At the Partner's request, AppXite shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Partner may take into account relevant certifications held by AppXite.

(e) The Partner may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of AppXite and shall, where appropriate, be carried out with reasonable notice.

(f) The Parties shall make the information referred to in this DPA, including the results of any audits, available to the competent Supervisory Authority on request.

(g) AppXite shall maintain a record of all categories of Processing activities carried out on behalf of the Partner. AppXite 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.

(h) AppXite 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 AppXite shall accept to make any changes and amendments to this DPA that are required under Applicable Data Protection Law.

4.7. **Use of Sub-Processors**

(a) The Partner agrees that companies listed in the Annex I of this DPA are used as sub-processors under this DPA.

(b) The Partner has the AppXite's general authorization for the engagement of sub-processors from an agreed list. When the AppXite engages a new subcontractor, AppXite shall give Partner notice by updating this DPA or otherwise making this information available to Partner at least one (1) month in advance, thereby giving the Partner sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The AppXite shall provide the Partner with the information necessary to enable the Partner to exercise the right to object.

(c) Where AppXite engages a sub-processor for carrying out specific processing activities (on behalf of the Partner), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the AppXite in accordance with this DPA. AppXite shall ensure that the sub-processor complies with the obligations to which the AppXite is subject pursuant to this DPA and the Applicable Data Protection Law. The AppXite shall remain fully responsible to the Partner for the performance of the sub-processor's obligations in accordance with its contract with the AppXite. AppXite shall notify the Partner of any failure by the sub-processor to fulfil its contractual obligations.

(d) At the Partner's request, AppXite shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Partner. To the extent necessary to protect business secret or other confidential information, including personal data, the AppXite may redact the text of the agreement prior to sharing the copy.

(e) The AppXite shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the AppXite has factually disappeared, ceased to exist in law or has become insolvent - the Partner shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

4.8. **International Transfers**

(a) Any transfer of data to a third country which is not listed in the Annex I this DPA or an international organization by AppXite shall be done only on the basis of documented instructions from the Partner or in order to fulfil a specific requirement under the Applicable Data Protection Law to which AppXite is subject and shall take place in compliance with Chapter V of the GDPR.

(b) The Partner agrees that where AppXite engages a sub-processor in accordance with Section 4.7. (a) for carrying out specific processing activities (on behalf of the Partner) and those processing activities involve a transfer of personal data within the meaning of Chapter V of GDPR, the AppXite and the sub-processor can ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the EU Commission in accordance with of Article 46(2) of the GDPR, provided the conditions for the use of those standard contractual clauses are met.

4.9. **Assistance to the Partner**

(a) AppXite shall, taking into account the nature of the processing, assist Partner by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Partner's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

(b) If AppXite receives a request from a data subject to exercise one or more of its rights under the GDPR in connection with the Platform and/or Services for which AppXite is a data processor or sub-processor, AppXite will promptly notify the Partner for Partner to address such request directly, e.g. by using the Platform functionality. AppXite shall comply with reasonable requests by Partner to assist with Partner's response to such a data subject request.

(c) AppXite shall assist the Partner in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), AppXite shall comply with the Partner's instructions.

(d) In the event that competent authorities or any other third parties request information from the AppXite regarding the Processing of Personal Data covered by this DPA, AppXite shall refer such request to the Partner. AppXite may not in any way act on behalf of or as a representative of the Partner.

(e) In addition to the AppXite's obligation to assist the Partner pursuant to Section 4.9 (b), the AppXite shall furthermore assist the Partner in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to AppXite:

- the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
- the obligation to consult the competent Supervisory Authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Partner to mitigate the risk;
- the obligation to ensure that Personal Data is accurate and up to date, by informing the Partner without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated.

(f) The Security and Compliance Whitepaper specifies the appropriate technical and organisational measures by which AppXite is required to assist the Partner in the application of this Section as well as the scope and the extent of the assistance required.

4.10. **Personal Data Breach Notification.**

(a) In case of a Personal Data Breach involving Personal Data Processed on behalf of the Partner the AppXite shall, taking into account the nature of Processing and the information available to AppXite, assist the Partner in ensuring compliance with the Partner's obligations pursuant to Articles 33 and 34 in the GDPR. Further the AppXite shall notify the Partner without undue delay, but not later than twenty-four (24) hours after becoming aware of such a Personal Data Breach. The notification shall at least:

a. 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;

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

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

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

(b) Partner shall notify AppXite promptly if Partner becomes aware of any Personal Data Breach or compromised authentication credentials.

5. BREACH OF DPA, TERM AND TERMINATION

(a) Without prejudice to any provisions of GDPR, in the event that AppXite is in breach of its obligations under this DPA, the Partner may instruct the AppXite to suspend the processing of personal data until the latter complies with this DPA or the Agreement is terminated. AppXite shall promptly inform the Partner in case it is unable to comply with this DPA, for whatever reason.

(b) The Partner shall be entitled to terminate the Agreement insofar as it concerns processing of personal data in accordance with the terms of this DPA if:

a. the processing of Personal Data by the AppXite has been suspended by the Partner pursuant to point (a) and if compliance with this DPA is not restored within a reasonable time and in any event within one (1) month following suspension;

b. AppXite is in substantial or persistent breach of this DPA or its obligations under the Applicable Data Protection Law;

c. AppXite fails to comply with a binding decision of a competent court or the competent Supervisory Authority regarding its obligations pursuant to this DPA or Applicable Data Protection Law.

(c) The AppXite shall be entitled to terminate the Agreement insofar as it concerns processing of personal data under this DPA where, after having informed the Partner that its instructions infringe applicable legal requirements in accordance with Clause 4.2 (b), the Partner insists on compliance with the instructions.

(d) Following termination of the Agreement, AppXite shall, at the choice of the Partner, delete all Personal Data processed on behalf of the Partner and certify to the Partner that it has done so, or return all the Personal Data to the Partner and delete existing copies unless Applicable Data Protection Law requires storage of the personal data. Until the data is deleted or returned, AppXite shall continue to ensure compliance with this DPA.

6. CONTACT DETAILS

Email: dpo@appxte.com

Attn: Īlajs Lijs

Mailing address:

- SIA "AppXite"
- Reg.No.: 40003843899
- Address: Matrozu street 15, Rīga, Latvia, LV-1048
- Attn: DPO

Annex I to the Data Processing Agreement
Processing Details

AppXite as Processor

Purposes of processing	Provision of the Platform (including providing personalized user experience) and Services pursuant to the Agreement.
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).

AppXite as Controller

Purposes of processing	Incident Resolution, troubleshooting, and further development of the Platform, internal incident and security reporting, compliance with legal obligations
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
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).

Annex II to the Data Processing Agreement
CCPA provisions

The following provisions apply to processing of Personal Information in relation to California residents:

1. Definitions and Interpretations

ii. "**Personal information**" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Consumer or household as defined in the CCPA;

iii. "**CCPA**" shall mean the US California Consumer Privacy Act of 2018, as amended from time to time;

iv. "**Consumer**" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

2. AppXite Obligations

i. AppXite shall not retain, use, or disclose the Personal Data: (i) for any purpose other than for the specific purpose of performing the services set forth in the Agreement or as otherwise permitted by the CCPA and its implementing regulations; (ii) for a commercial purpose other than providing the services specified in the contract with the business; or (iii) outside the direct business relationship between the person and AppXite;

ii. AppXite shall not sell Personal Information;

iii. AppXite shall encrypt all Personal Information at rest and apply other appropriate organizational and security measures required to safeguard Personal Information;

iv. AppXite will cooperate with Partner in order to efficiently, effectively, and timely respond to requests from individuals related to the Personal Data. These requests include, but are not limited to, requests to review, correct, amend or delete Personal Information. Consumer requests shall be sent to dpo@appxite.com. AppXite shall respond, free of charge, within thirty (30) business days, in an electronic format.

AppXite may refuse to delete personal information in the event such personal information is required to: (i) Detect security incidents; (ii) protect against malicious, deceptive, fraudulent, or illegal activity; (iii) Debug to identify and repair errors that impair existing intended functionality; (iii) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code; (iv) To enable solely internal uses that are reasonably aligned with the expectations of the Consumer based on the Consumer's relationship with the business; (v) Comply with a legal obligation; (vi) Otherwise use the Personal Information, internally, in a lawful manner that is compatible with the context in which the Consumer provided the information.