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 a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- "***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	Name, surname, email address, employment details (company, job title), IP address.
Categories of data subjects	Platform end-users (contractors/employees of the Partner and its sellers/end-customers).
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, SendGrid, Zendesk
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	Name, surname, email address, employment details (company, job title), IP address.
Processing operations/activities	Platform end-users (contractors/employees of the Partner and its sellers/end-customers).
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.

Standard Contractual Clauses

Section I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

[INTENTIONALLY OMITTED]

SECTION II – OBLIGATIONS OF THE PARTIES

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least

implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

a. The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

c. The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

a. The Parties shall be able to demonstrate compliance with these Clauses.

b. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred

personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[1];

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

[1] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiency representative time-frame. This refers in particular to internal records or documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or application of the law in practice, such as case law and reports by independent oversight bodies.

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Netherlands.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Netherlands.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Netherlands.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

- **Name (Customer):** Partner company name as indicated in the relevant Order Form.
- **Address:** Legal address as indicated in the relevant Order Form.
- **Contact person's name, position and contact details:** signatory as indicated in the relevant Order Form.
- **Activities relevant to the data transferred under these Clauses:** Data exporter's use of AppXite Platform and ancillary services as detailed in one or more Order Form(s) to process Personal Data in accordance with the terms of the Partner Agreement and the Data Processing Agreement.
- **Signature and date:** These Standard Contractual Clauses shall be an integral part of the Partner Agreement.
- **Role (controller/processor):** Controller.

Data importer(s):

- **Name:** AppXite Ltd.
- **Address:** Matrozu street 15, Riga, LV-1048, Latvia
- **Contact person's name, position and contact details:** DPO, dpo@appxite.com
- **Activities relevant to the data transferred under these Clauses:** Provision of data importer of AppXite Platform and ancillary services upon the instruction of the data exporter in accordance with the terms of the Partner Agreement and the Data Processing Agreement.
- **Role (controller/processor):** Processor
- **Signature and date:** These Standard Contractual Clauses shall be an integral part of the Partner Agreement.

A. LIST OF PARTIES

MODULE FOUR: Transfer processor to controller

Data exporter(s):

- **Name:** AppXite Ltd.
- **Address:** Matrozu street 15, Riga, LV-1048, Latvia
- **Contact person's name, position and contact details:** DPO, dpo@appxite.com

- **Activities relevant to the data transferred under these Clauses:** Provision of data importer of AppXite Platform and ancillary services upon the instruction of the data exporter in accordance with the terms of the Partner Agreement and the Data Processing Agreement.
- **Role (controller/processor):** Processor
- **Signature and date:** These Standard Contractual Clauses shall be an integral part of the Partner Agreement.

Data importer(s):

- **Name (Customer):** Partner company name as indicated in the relevant Order Form.
- **Address:** Legal address as indicated in the relevant Order Form.
- **Contact person's name, position and contact details:** signatory as indicated in the relevant Order Form.
- **Activities relevant to the data transferred under these Clauses:** Data exporter's use of AppXite Platform and ancillary services as detailed in one or more Order Form(s) to process Personal Data in accordance with the terms of the Partner Agreement and the Data Processing Agreement.
- **Signature and date:** These Standard Contractual Clauses shall be an integral part of the Partner Agreement.
- **Role (controller/processor):** Controller.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

- Platform end-users (contractors/employees of the Partner and its sellers/end-customers).

Categories of personal data transferred

- Name, surname, email address, employment details (company, job title), IP address.

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

Continuous basis.

Nature of the processing

Collection, disclosure, use, erasure.

Purpose(s) of the data transfer and further processing

Delivery of the AppXite Platform and related services pursuant to the Partner Agreement, Purposes of processing include but are not limited to: User authentication, logging, user management, platform activity notification (e.g. order placement, new user being added).

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

See. Sec.14.4.5 of the Partner Agreement. Criteria: Term of the Partner Agreement, Statute of Limitation.

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

See. Annex III

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

Valsts Datu Inspekcija

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE FOUR: Transfer processor to controller

Description of the technical and organisational measures implemented by the AppXite:

- **Network Security.** The network security measures include firewall, network access control, network vulnerability management, use of VPN, network encryption;
- **Hosting Infrastructure.** AppXite hosts its services in geographically distributed and secure cloud data centres provided by Microsoft. The data is replicated across multiple data centres in EEA to ensure the best performance, security and business continuity.
- **Monitoring.** AppXite has implemented the monitoring solutions designed for threat detection.
- **Access control.** Access to the Data is managed through a technical system for authorization control based on the "need-to-know" basis and "least privilege" principle.
- **Sub-Processor security.** Prior to engaging a sub-processor that process any portion of personal data, AppXite performs a sub-processor security vetting to ensure that a sub-processor provides a level of security appropriate to their access to the personal data.
- **Dedicated Security Team.** AppXite has a dedicated security team which assists in handling data security incidents and data subjects' requests.
- **Policies and Procedures.** AppXite ensures that all of its data processing activities are performed according to the established policies, that include but are not limited to: Information Security Policy, Access Management Policy, Employee Code of Conduct, Encryption Policy, Incident Management Policy, Data Breach Notification Policy, Change Management, Disaster Recovery.
- **Code Review.** AppXite has implemented a code review process to improve the security of the code used for the purposes of the Platform. The code is being subject to security testing prior to being released in production. Code level security vulnerabilities are being scanned on a periodic basis.

- **Encryption.** All personal data is classified as strictly confidential and subject to encryption in transit. Considering that data may be intercepted in transit or monitored as plaintext data transmitted across unencrypted network, any transfer of data through a network is encrypted according to the industry-accepted encryption mechanism TLS 1.2. Monitoring tools are implemented to detect any malicious attempt to access customer data.
- **Third party certifications.** AppXite maintains the compliance with the ISO standard pertaining to information security, including: ISO 27001, ISO 27017, ISO 27018.
- Other technical and organizational measures as detailed in the AppXite Information Security and Compliance Whitepaper.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The controller has authorized the use of the following sub-processors:

Sub-Processor	Purpose and Description of Processing	Data Storage Location
Microsoft Operations Ireland Ltd	Infrastructure hosting. Ticket escalation. Processing includes collection, storage, use, disclosure.	EU/EEA
Auth0	User authentication. Processing includes collection, storage, use, disclosure.	EU/EEA
SendGrid	Email messaging service. Processing includes collection, storage, use, disclosure.	EU/EEA
Zendesk	Support ticketing system. Processing includes collection, storage, use, disclosure.	EU/EEA