Data Processing Agreement (DPA)

This Data Processing Agreement (DPA) is an addendum to the Xapi End User License Agreement ("EULA") and is made between:

- **User or Subscriber (PII Controller):** The entity or individual who uses or subscribes to Xapi, accepts the EULA, and acts as the PII Controller for the PII being processed (hereafter referred to as the **"Customer"** in this DPA).

- **X-venture: X-venture Global Solutions Pvt Ltd**, registered in Sri Lanka bearing registration number: PV00233880, with its principal place of business at No 1185/1/E, Vidyala Junction, Pannipitiya, Sri Lanka, which acts as the PII Processor.

This DPA is designed to ensure X-venture's compliance with the specific requirements of ISO/IEC 27018:2019 for the protection of Personally Identifiable Information (PII) in the public cloud environment.

DPA Execution Instructions

1. **DPA Status:** This Data Processing Agreement is a single, complete document.

2. **X-venture Acceptance:** This DPA has been pre-signed by an authorized representative on behalf of X-venture (the PII Processor) and is hosted on X-venture's website.

3. **Customer Acceptance (Standard Customer):** For the majority of users, this DPA is legally executed and binding upon the Customer's acceptance of the Xapi End User License Agreement (EULA), which incorporates this DPA by reference. No further action is required.

4. **Manual Execution (Enterprise Only):** If the Customer's internal compliance policy requires a physically counter-signed copy, the Customer must:

   a. Complete the information in the Customer signature box and sign on the final page.

   b. Send the complete, manually signed DPA to X-venture by email (PDF format preferred) to the designated Data Protection Officer (DPO): dpo@x-venture.io

1. Scope, Purpose, and Use Limitation

1.1. Scope of PII

The PII processed under this DPA is strictly limited to Account Information-related PII: Full Name, Email Address, Profile Picture, User Name, Website, Company, Country, Timezone and associated authentication data necessary for the Customer's use of X-venture's SaaS product, Xapi.

1.2. Purpose Limitation

X-venture shall process PII solely for the purpose of providing the contracted SaaS services (account creation, authentication, service delivery, billing) and shall not process PII for any purpose independent of the Customer's instructions without the Customer's prior documented consent.

1.3. Commercial Use Restriction

X-venture guarantees that PII shall not be used for marketing, advertising, or profiling without the PII Principal's express, non-conditional consent. The granting of consent for commercial use shall never be a condition for receiving the contracted service.

2. PII Principals' Rights and Cooperation

2.1. Cooperation on PII Rights

X-venture shall provide the Customer with the means (technical tools and informational guidance) necessary to enable the Customer to fulfil its obligation to facilitate the PII Principal's rights to access, correct, and/or erase PII about them.

2.2. Customer Access and Portability

X-venture guarantees that the Customer shall be provided with the necessary facilities to retrieve a copy of their processed PII (Account Data) for data portability or other legal exit requirements.

3. Sub-processing and Data Location

3.1. Disclosure of Sub-processors

X-venture shall disclose the use and identity of all subcontractors processing PII to the Customer before their engagement. This information shall include the services they provide, the PII they process, and the countries in which PII can be stored.

3.2. Geographical Location

X-venture shall document the countries in which PII is stored. X-venture shall inform the Customer in a timely fashion of any intended changes to the geographical location of PII storage, allowing the Customer the ability to object to such changes or terminate the agreement.

3.3. Flow-Down Contractual Measures

Contracts between X-venture and any subcontractors processing PII shall mandate technical and organizational measures that meet or exceed X-venture's PII protection obligations under this DPA. Such security measures shall not be subject to unilateral reduction by the subcontractor.

4. Security, Access Control, and Segregation

4.1. Confidentiality and Training

All individuals under X-venture's control with access to PII shall be subject to a confidentiality obligation that survives termination of their employment or contract. X-venture further guarantees that staff training includes specific PII breach awareness and the legal/disciplinary consequences of non-compliance.

4.2. Management of User IDs

X-venture shall ensure that all individuals accessing stored PII have a distinct User ID for identification and authentication. Deactivated or expired user IDs shall not be granted to other individuals.

4.3. Records of Authorized Users

X-venture shall maintain an up-to-date record of authorized users or user profiles who have access to the information system containing PII.

4.4. Segregation of PII

X-venture shall implement and maintain controls for physical and logical segregation of the Customer's PII in the multi-customer cloud environment. X-venture shall also implement controls to ensure that PII is not accessible on pre-used data storage space that has been reassigned.

4.5. Data in Transit

PII transmitted over public data-transmission networks shall be encrypted prior to transmission. Controls shall be implemented to ensure the PII reaches its intended destination.

4.6. Media Leaving Premises

PII on media leaving X-venture's premises shall be authorized and encrypted. Unencrypted portable physical media shall not be used for PII unless unavoidable and documented.

4.7. Secure Log-on Procedures

X-venture shall provide and maintain secure log-on procedures for all Customer accounts used to access the cloud service and its administrative components (e.g., strong password policies, multi-factor authentication capability).

4.8. Security Measures Guarantee

X-venture guarantees that the security controls and protection measures defined within this DPA shall not be unilaterally reduced or degraded by X-venture throughout the term of the EULA without the Customer's express written agreement.

5. Security Incidents and Legal Disclosure

5.1. Breach Notification and Incident Handling

X-venture shall promptly notify the Customer of any unauthorized access, loss, disclosure, or alteration of PII. X-venture guarantees that its incident process includes a step to immediately determine if a data breach involving PII has taken place. Notification shall include the necessary details for the Customer to fulfil its obligation to notify relevant authorities and PII principals.

5.2. Legal Disclosure Notification

X-venture shall notify the Customer of any legally binding request for the disclosure of PII by a law enforcement authority, unless legally prohibited. X-venture further commits to rejecting any request for PII disclosure that is not legally binding and, where not prohibited, shall first refer the third party to the Customer or seek the Customer's written authorization before any disclosure.

5.3. Recording of Disclosures

X-venture shall maintain a formal log and record of all disclosures of PII to third parties, noting what PII was disclosed, to whom, and when.

5.4. Data Protection Officer

For all data protection inquiries, audit requests, and formal breach notifications, the Customer shall contact X-venture's designated Data Protection Officer (DPO) via the following channel:

Email: dpo@X-venture.io

Address: X-venture Global Solutions Pvt Ltd *(Attention: Data Protection Officer)*

6. PII Disposal and Audit Assurance

6.1. Termination and Disposal

Upon contract termination, X-venture shall, at the Customer's choice, securely erase, return, or transfer all PII. X-venture shall provide the Customer with the necessary information to ensure PII is erased from backups and subcontractor systems.

6.2. Erasure of Temporary Files and Backups

X-venture shall implement a procedure for the secure erasure of temporary files and documents containing PII within a specified period. X-venture shall maintain a policy for the secure erasure of PII contained within information held for backup purposes.

6.3. Secure Media Handling

X-venture's default practice is not to create hardcopy material containing PII. In the exceptional event that hardcopy material displaying PII is created, X-venture guarantees that:

1. Procedures are in place to restrict and document such creation.
2. All PII-containing hardcopy materials shall be securely destroyed immediately after use.

6.4. Data Restoration Logging

X-venture shall maintain a procedure and log of all data restoration efforts, including the person responsible, the description of the restored data, and details of any manually restored data.

6.5. Independent Review

Where necessary, X-venture shall provide the Customer with independent evidence (e.g., ISO/IEC 27001:2022 or ISO 27018:2019 certificates) that information security and PII protection are implemented and operated correctly to satisfy the Customer's right to audit.

6.6. Policy Retention

X-venture shall retain copies of security policies and operating procedures related to PII processing for a specified, documented period after they are replaced or updated.

Acceptance

By executing the main Terms of Service (EULA), X-venture and the Customer agree to the terms of this Data Processing Agreement.

X-venture (PII Processor)

Signature: _____

Name: _____

Title: _____

Date: _____

Customer (PII Controller)

Signature: _____

Name: _____

Title: _____

Date: _____