WALLET PARTNER ADDENDUM

Last updated: 11 January 2024

This addendum (the "Addendum"), in addition to the Terms and Conditions found in https://pdax.ph/terms-and-conditions, and all rules and policies incorporated therein by reference, shall govern your relationship with PDAX when creating, accessing, and using your PDAX Account for Wallet Services (as defined in this Addendum).

This Addendum is deemed an addition to, and incorporated into the Terms and Conditions. In case of conflict between the Terms and Conditions and this Addendum, this Addendum shall govern the activities and services considered as and related to the Wallet Services.

I. WALLET PARTNER AGREEMENT

1. DEFINITIONS

The capitalized terms used herein which are defined in the Terms and Conditions, shall have the respective meanings assigned to them in the Terms and Conditions except as otherwise provided herein or unless the context otherwise requires. In addition to the definitions in the Terms and Conditions, the following definitions apply:

a. **User's Clients** refers to specific individuals with a business relationship with the User, including senders and corresponding receivers of Digital Assets for whose benefit, the User avails of Services under the Terms and Condition and this Addendum.

b. **Wallet Services** refer to the Services made available through the PDAX Platform where the User is allowed to create a PDAX Account solely for the purposes of maintaining a Digital Asset Wallet in the PDAX Platform where the User can hold and store Digital Assets.

2. GENERAL POLICY

This Addendum governs your access and usage of the PDAX Platform and your PDAX Account solely for the Wallet Services.

PDAX may promulgate operational guidelines to govern the provision of Wallet Services, from time to time, which shall be deemed incorporated into, and shall form part of, this Addendum. Such additional technical and operational guidelines or any revisions to this Addendum shall be governed by [Section XX (Amendments and Revisions)] of the Terms and Conditions and any separate written amendments between you and PDAX.

3. WALLET SERVICE

You understand, agree and acknowledge that when you accede to this Addendum without acceding to additional PDAX Platform Rules (other than the Terms and Conditions), your use of the PDAX Platform will be limited to the Wallet Services, as follows:

a. You shall use the PDAX Platform, solely for storage of Digital Assets to your Digital Asset wallet maintained in the PDAX Platform.

b. You can only transfer in or transfer out Digital Assets to and from your PDAX Account to Third Party Accounts that you own and are under your name.

c. Unless you accede to additional applicable PDAX Platform Rules or execute additional agreements with PDAX, you are not permitted to avail of any other Service including using your PDAX Account for placing orders, trading, cashing in and cashing out in the PDAX Platform.. For the avoidance of doubt, all provisions in the Terms and Conditions allowing a User to trade, buy, or sell Digital Assets, or transfer Fiat Currency to and from a PDAX Account do not apply to you, and unless you accede to additional PDAX Platform Rules, provisions relating to Services (other than the Wallet Services) likewise do not apply to you.

d. If you are a licensed financial institution, you may use your PDAX Account to hold or store Digital Assets for and on behalf of User's Clients with the written approval of PDAX.

4. KYC PROTOCOLS

When the User uses the Digital Wallet in the User's PDAX Account to hold or store Digital Assets for and on behalf of User's Clients, the PDAX KYC Program and Procedures as contained in PDAX Terms and Conditions shall be equally applicable to the Wallet Services and this Addendum. To the extent allowed by Applicable Laws and Rules, PDAX may, at its sole and absolute discretion, opt to rely on the User to perform the required customer due diligence procedures. In any case, PDAX may, at its sole discretion, require the User to submit a sworn certification in a form to be provided by PDAX, and in addition, the User hereby undertakes and certifies that:

a. the User has conducted, is conducting, and will continue to conduct, the prescribed identification procedures for the User's Clients in accordance with the Applicable Laws and Rules, and the User's Money Laundering and Terrorist Financing Prevention Program, including face-to-face contact, personal interviews, and/or such Information and Communications Technology ("ICT") methods permitting customer identification in a similar manner, to validate the existence and establish the identity to establish the existence of the ultimate User's Clients;

b. if the standards of the country where the User is operating has User's Clients' identification process requirements which are less stringent than those of the Republic of the Philippines, the User shall follow the standards of the Republic of the Philippines, specifically with respect to customer due diligence, record keeping obligations, and the requirements prescribed in: (i) the AMLA and its Implementing Rules and Regulations; (ii) Part Nine of Q-Regulations (Anti-Money Laundering Regulations) of the MORNBFI, as may be amended from time to time; (iii) and related issuances of the BSP including but not limited to BSP Circular No. 706, as amended by BSP Circulars No. 950 and No. 1022 and as may be further amended from time to time (collectively, "Philippine AML/CTF laws");

c. upon request, the User shall inform PDAX of: (i) the level of country risk, for all jurisdictions where it operates; (ii) the nature of its business and reputation; (iii) entities responsible for, and the quality of, its supervision, regulation, and monitoring; and (iv) any money-laundering or terrorist financing investigation or regulatory action which it may have been involved in;

d. the User has measures in place to conduct due diligence and record-keeping requirements in relation to the User's Clients in accordance with all requirements of all regulations enforced by the regulatory bodies of all jurisdictions where it operates;

e. the User has conducted, and continues to conduct the required screening of its users or clients, including the User's Clients, against established sanctions lists, *i.e.* the "Specially Designated Nationals and Blocked Persons" list maintained by the Sanctions Authorities, or any similar list maintained by, or public announcement of Sanctions designation made by them, including, the "Specially Designated Nationals and Blocked Persons" list maintained by the OFAC, the Consolidated List maintained by the UNSC, the Consolidated List of Financial Sanctions Targets and the Investment Ban List maintained by HMT, those designated by the ATC, or any similar list maintained by, or public announcement of Sanctions designation made by, any of the Sanctions Authorities;

f. the User has not, does not, and will not endorse or allow its users (including the User's Clients), who is a positive match to any Sanctions, to access the PDAX Platform or avail of any Service, including the Wallet Service;

g. the User has not, at any time, been reprimanded or cited, or subject to regulatory examination or other similar actions on account of unsatisfactory, insufficient, inadequate Anti-money Laundering/Counter-Terrorist Financing policies, procedures or practices;

h. upon request, the User undertakes to provide PDAX with the identification documents of all of the User's Clients, including senders and receivers without delay. The User warrants that it has secured the consent of the User's Clients to share such information;

i. the User permits PDAX to conduct periodic KYC reliance & MLPP (or equivalent MLPP procedures) account reviews as PDAX sees fit, and undertakes to provide additional documentation, as may be necessary to fully accomplish reviews without delay.

The User acknowledges that PDAX has full discretion to terminate its Services, including the Waller Service, in case of fraud, misconduct, misrepresentation, or breach of the foregoing certifications; breach by the User or the User's Clients of applicable laws, rules, and regulations, including but not limited to the AMLA, or other related rules and regulations promulgated by the BSP; or to protect the legitimate interests of PDAX.

5. FEES

You may be charged fees different from those charged to regular PDAX Accounts, which will be made known to you before you are charged.

6. CONFIDENTIALITY AND DISCLOSURE OF INFORMATION

All information which is disclosed by PDAX to the User or by the User to PDAX shall be protected hereunder and considered as Confidential Information.

a. **Confidential Information.** For the purposes of this Section, "Disclosing Party" shall refer to the party disclosing the Confidential Information and

"Receiving Party" shall refer to the party receiving the Confidential Information.

"Confidential Information" means all non-public, confidential or proprietary communications or data, in any form, whether tangible or intangible, which are disclosed or furnished through whichever medium by any director, officer, employee, agent, or consultant (collectively, the "Representatives") of any department or business area of the Disclosing Party hereto, including their Affiliates, to the Receiving Party, its Affiliates, and their Representatives, and which are to be protected hereunder against unrestricted disclosure or competitive use by the Receiving Party. The following are also Confidential Information:

(i) Technical information, which refers to methods, processes, formulae, compositions, inventions, machines, computer programs, and research projects.

(ii) Business information, which refers to customer lists; pricing data sources of supply; marketing, production, or merchandising systems or plans; and all information or material that has or could have commercial value or other utility in the business of the Disclosing Party.

(iii) Personal Information, which refers to any information, whether recorded in a material form or not, from which the identity of an individual, including but not limited to the Disclosing Party's applicants, agents, employees, officers, directors, consultants, clients, customers, suppliers, service providers, and partners, is apparent or can be reasonably and directly ascertained, or when put together with other information would directly and certainly identify such individual. This includes but is not limited to such individual's name, race, ethnic origin, age, place and date of birth, citizenship, residence or office address, contact info (phone and/or email address), marital status, name of spouse and/or child/children/dependents, if any, name of parents, physical attributes or identifying marks, occupation, religious, philosophical or political affiliations, education, health, previous or current health records, criminal background or any proceeding for any offense or court sentences, social security numbers, PhilHealth number and details, Pag-Ibig number and details, Tax Identification No. and details, tax returns, licenses or its denials, suspension or revocation, or any similar information or data protected under the DPA and Applicable Laws and Rules.

(iv) Information ought reasonably to be treated as proprietary, commercially sensitive or confidential considering the surrounding circumstance, including those that has been derived or created from any Confidential Information.

Confidential Information excludes:

(i) information that becomes generally available to the public other than as a result of the disclosure by the Receiving Party in violation of this Addendum;

(ii) information available or made available to a Receiving Party on a non-confidential basis prior to disclosure by the Disclosing Party;

(iii) only to such court, tribunal, regulatory authority or entity authorized to request for disclosure, information that is required to be disclosed by any court, tribunal, or regulatory authority or by any requirement of law, legal process, regulation, or governmental order, decree, or rule, or necessary or desirable for a Party to disclose in connection with any proceeding in any court, tribunal or before any regulatory authority in order to preserve its rights;

(iv) information that the Disclosing Party expressly agrees in writing to be disclosed by the Receiving Party to third parties;

(v) information lawfully received by the Receiving Party from an independent third party without any restriction and without any obligation of confidentiality;

(vi) information disclosed without restriction by the Disclosing Party to any third party; and

(vii) information which is independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information.

b. Restrictions on the Use of Confidential Information.

(i) The Receiving Party agrees, for itself, its affiliates, and their respective authorized representatives, to (a) hold all Confidential Information (regardless of whether it is specifically marked confidential or not) in strict confidence; (b) transmit the Confidential Information only to its representatives, its affiliates, and its affiliates' representatives, on a 'need-to-know' basis and after each one of them has agreed to be bound by these Addendum and not to disclose the same except as provided herein; (c) not to directly or indirectly use, copy, digest, or summarize any Confidential Information except as provided in these Addendum, and (d) not to disclose any Confidential Information to any third party without the prior written consent of the Disclosing Party. In the event that the Receiving Party becomes aware that Confidential Information has been disclosed to or accessed by any unauthorized party, the Receiving Party shall immediately notify the Disclosing Party thereof and shall take all appropriate countermeasures against further disclosure and to prevent or stop suspected or actual breaches of these Addendum.

(ii) The Receiving Party shall strictly comply with any and all Applicable Laws and Rules, including but not limited to the DPA, as well as any policy, measures, rules, and regulations of the Disclosing Party implementing such applicable laws and rules. The Receiving Party understands and agrees that the Disclosing Party shall have no liability for any of the Receiving Party's acts or omissions which may be in violation of such applicable laws and rules as well as the Disclosing Party's rules.

(iii) The Disclosing Party may grant its consent for the disclosure of the Confidential Information in its sole discretion and on a case-to-case basis. The Receiving Party expressly agrees not to use the Confidential Information to gain or attempt to gain a competitive advantage over the Disclosing Party. If requested by the Disclosing Party, the Receiving Party shall acknowledge receipt of any Confidential Information by signing receipts, initialing documents, or any other means that the Disclosing Party may reasonably request.

(iv) The Receiving Party will not permit copies of the Confidential Information to be made without the express written consent of the Disclosing Party. Copies shall be deemed confidential and, in all respects, subject to the terms of these Addendum

(v) If the Receiving Party is requested by a governmental entity to disclose any Confidential Information, it will promptly notify the Disclosing Party to allow the Receiving Party to do so. The Receiving Party will also cooperate in the Disclosing Party's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be afforded the Confidential Information. If in the absence of a protective order and the Receiving Party is compelled as a matter of law to disclose the Confidential Information, based upon the written opinion of the Receiving Party addressed to the Disclosing Party, the Receiving Party may disclose to the Party compelling the disclosure only the part of the Confidential Information as required by law to be disclosed. The Receiving Party will advise and consult with the Disclosing Party as to such disclosure and the nature and wording of such disclosure and the

Receiving Party will use its best efforts to obtain confidential treatment therefore.

c. **Property Rights and Ownership.** All Confidential Information, unless otherwise specified in writing, shall remain the sole and exclusive property of the Disclosing Party. The Disclosing Party retains ownership, including intellectual property rights, over all preexisting materials, documents and work originally created by it. The ownership over any materials, documents and work resulting collaboration with and through the joint efforts of the Parties shall be subject to the terms of definitive agreements to be negotiated by the Parties. No other rights, and particularly no license and no assignment of intellectual property rights including copyright, patent rights, design rights, trademarks, and mask work protection rights are implied or granted under this Agreement. The Parties shall not make use of the existence of any bilateral business relationship between them for the purpose of their own advertisement.

d. **Safekeeping.** The Receiving Party shall use the same care to avoid disclosure or unauthorized use of the Confidential Information as it uses to protect its own Confidential Information, but in no event less than reasonable care. It is agreed that:

(i) All Confidential Information shall be retained by the Receiving Party in a secure place with access limited only to the Receiving Party's Representatives who need to know such information for purposes of this Agreement; and

(ii) Confidential Information will be disclosed only to each Party's Representatives on a 'need-to-know' basis. It may be disclosed to third party consultants or advisers only with the prior consent of the Disclosing Party. In the event of such disclosure to any third party, the Receiving Party shall remain liable for any unauthorized disclosure by such person or entity.

The Receiving Party shall ensure that all of its representatives, affiliates, and third-party consultants having access to Confidential Information adhere to the terms and conditions of these Addendum as if they were Parties hereto.

All confidentiality obligations contemplated under this Section shall be coterminous with the permission duration as stated in the PDAX Permission and one (1) year thereafter.

7. REPRESENTATIONS AND WARRANTIES OF THE USER

The User hereby represents and warrants to PDAX that each of the following statements are true, accurate and correct as to the User, and as to each of the User’s Clients:

a. each of the User and User's Client has full power, authority and legal capacity to (i) access and use the PDAX Platform and/or avail of the Wallet Services and (ii) enter into and deliver, and perform your obligations under the Terms and Conditions, this Addendum, and any agreement entered into pursuant to, or in connection with, the Terms and Conditions, this Addendum, or the use of the PDAX Platform for, and/or availment of, the Conversion, as may be applicable, and the Wallet Services;

   If the User or the User's Client is an individual or a natural person, he or she has all the legal and mental capacity and rights to avail of the Conversion, as may be applicable, and the Wallet Services, under all Applicable Laws and Rules.

   If the User or the User's Client is a corporation, partnership or a juridical entity or person, it is duly organized, validly existing and in good standing as a corporation, partnership or any other entity as represented under the laws and regulations of the country exercising jurisdiction over your incorporation, organization or chartering;

b. each of the User and User's Client is not a resident of (or incorporated in), and will not be availing of the Conversion, as may be applicable, and the Wallet Services, from, an unsupported jurisdiction or a jurisdiction where availing of Conversion, as may be applicable, and the Wallet Services, are prohibited by Applicable Laws and Rules;

c. each of the User and User's Client has not been previously suspended or prohibited from: (i) maintaining a PDAX Account; (ii) being a user of the PDAX Platform; or (iii) availing of the Services.

d. All agreements, documents, contracts and ancillary forms which require User’s or User's Client’s signature or consent is duly signed and executed by authorized signatories or representatives by the User or the User's Client, as may be applicable, and as such each of such agreements, documents, contracts and ancillary forms constitutes a legal, valid, and binding obligation of the User or the User's Client, as the case may be; and

e. User has obtained and effected all consents, approvals and authorizations from Regulatory Authorities that are necessary for the User’s or the User's Client’s due execution, delivery, and performance of its obligations under this Addendum.

8. INDEMNITY AND LIMITATIONS OF LIABILITY

In addition to Section 17 (Limitation of Liability) and Section 18 (Indemnity) of the PDAX Terms and Conditions, applicable Platform Rules and unless as otherwise provided in a separate written agreement, User agrees to fully defend, hold harmless, and indemnify PDAX or the PDAX Group from and against all claims, disputes, settlements, awards, damages, losses, expenses and costs (including legal costs) suffered or incurred by PDAX or the PDAX Group in connection with or arising from:

a. User’s or the User's Client’s breach of its obligations or warranties or inaccuracy of its representations as conformed or incorporated in this Addendum, PDAX Terms and Conditions, Privacy Policy, all applicable PDAX Platform Rules and other relevant documents and communications;
b. any claim or dispute between and among the User, the User's Client and any third person arising from or in connection with the use of the PDAX Platform or availment of the Conversion, as may be applicable, and the Walet Services by the User unless such claim is solely caused by the breach of this Addendum, or fraud by PDAX. Disputes between and among the User, the User's Client and any third person as to Wallet Services shall be resolved solely between or among them; and
c. any claim, damages, penalties or expenses arising from or in connection with any violation of any Applicable Laws and Rules of the User or the User's Client.

To the extent allowed by Applicable Laws and Rules, User hereby agrees to fully defend, hold harmless, and indemnify PDAX and the PDAX Group, from and against all claims, disputes, settlements, awards, damages, losses, expenses and costs (including legal costs) suffered or incurred by PDAX and the PDAX Group, in connection with or arising from PDAX use of information materials provided by the User, pursuant to this Addendum and the provision of the Conversion, as may be applicable, and the Wallet Services.

II. DATA OUTSOURCING AGREEMENT

The User shall abide by all Applicable Laws and Rules in relation to personal data processing and the Privacy Policy.

To the extent that PDAX could potentially process the Personal Data of the Beneficiaries in relation to the Conversion, as may be applicable, and the Wallet Services as defined herein, this Data Outsourcing Agreement (the "Sub-Agreement") is made and executed by and between the User and PDAX.

RECITALS:

a. The Parties have agreed to enter into an agreement wherein the User has opened a PDAX Account, solely for the Wallet Service;

b. During the course of the User's usage of the PDAX Account and availment of the Services, it is understood that Digital Assets transferred to, or withdrawn from, the PDAX Account, may constitute an aggregated sum composed of various sums pertaining to a User's Client;

c. PDAX could potentially process the Personal Data of the User's Clients or any relevant individual as may be required by Applicable Laws and Rules in relation to the Wallet Service; and

d. The Parties agree that the User is the Personal Information Controller and PDAX is the Personal Information Processor, as defined in the DPA.

NOW, THEREFORE, for and in consideration of the foregoing premises and mutual covenants stated hereunder, PDAX and User hereto agree as follows:

a. **Term** – This Sub-Agreement shall have the duration indicated in the DOD (as defined herein).

b. **Adherence to the Data Privacy Act of 2012** – The Parties hereby adhere to the DPA, recognizing the importance of appropriate privacy protections for data subjects.

c. **Definitions**

(i) DOD refers to the data outsourcing details, to be executed separately by the Parties, which contains the subject matter of processing, duration of processing, purposes of processing, Data Subjects and

Personal Data types, geographic location of processing, and details of the arrangement between PDAX and the User.

(ii) Personal Information refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

(iii) Sensitive Personal Information refers to personal information:

- About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
- Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- Specifically established by an executive order or an act of Congress to be kept classified.

(iv) Personal Data refers to personal information, sensitive personal information, and privileged information.

(v) Processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.

(vi) Data Outsourcing is the disclosure or transfer of Personal Data by a Personal Information Controller to a Personal Information Processor.

(vii) DPA means Republic Act 10173, also known as, Data Privacy Act of 2012, its Implementing Rules and Regulations, and the issuances of the National Privacy Commission.

(viii) Data Protection Officer is any individual/s designated by the Personal Information Controller or Personal Information Processor who is accountable for compliance with the DPA.

(ix) Data Subject refers to an individual whose personal, sensitive personal, or privileged information is processed.

(x) Security Incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.

(xi) Personal Data Breach' refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

- An availability breach resulting from loss, accidental or unlawful destruction of personal data;
- Integrity breach resulting from alteration of personal data; and/or
- A confidentiality breach resulting from the unauthorized disclosure of or access to Personal Data.

(xii) Personal Information Controller refers to a natural or juridical person, or any other body who controls the processing of Personal Data, or instructs another to process Personal Data on its behalf. The term excludes:

- A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
- A natural person who processes personal data in connection with his or her personal, family, or household affairs

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.

(xiii) Personal Information Processor refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of Personal Data pertaining to a Data Subject.

(xiv) Technical, Physical, and Organizational Security Measures, or TPOSM means those measures aimed at protecting Personal Information transmitted, stored, or otherwise processed against improper, unauthorized, accidental or unlawful processing, destruction or loss, disposal, alteration, disclosure, or access, and against all other unauthorized and unlawful forms of processing.

d. **Roles of the Parties** – User is the Personal Information Controller of the Personal Data disclosed to PDAX. PDAX is a Personal Information Processor, i.e., it processes such Personal Data upon the instruction of the User.

In the event that either party takes on the role of a Personal Information Controller or Personal Information Processor, as defined under the DPA, such party herein undertakes to implement the necessary measures, and execute its role as Personal Information Controller or Personal Information Processor, as the case may be, in relation to any Personal Data which comes into its possession by virtue of the Terms and Conditions and this Addendum, in accordance with the DPA.

e. **Personal Data to be Collected and Processed** – PDAX shall process only the Personal Data listed in the DOD, in accordance with the terms of this Sub-Agreement.

The terms of this Sub-Agreement shall apply to Personal Data in all its forms. It may be on paper, stored electronically, held on film, microfiche, or other media. It includes text, pictures, audio, and video. It covers information transmitted by post, by electronic means, and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the data from creation, collection, storage, utilization, to disposal. The terms of this Sub-Agreement apply to all officers, employees, and clients of both Parties where they are performing their duties in relation to this Sub-Agreement.

f. **Purposes of Processing** – PDAX shall process the Personal Data only for the purposes listed in the DOD.

The User may, at any time and upon written instructions to PDAX, require PDAX to process the Personal Data pursuant to and consistent with the following purposes:

(i) Comply with statutory and regulatory requirements, including directives, issuances by, or obligations of User to any competent authority, regulator, supervisory body, enforcement agency, exchange, court, quasi-judicial body, or tribunal;

(ii) Enable User to exercise sound corporate governance over its businesses, ensure that risks arising therefrom are duly identified, measured, managed and mitigated, and enhance risk assessment and prevent fraud;

(iii) Enable User to conduct User audits or investigate a complaint or security threat;

(iv) Other legitimate business purposes of the User and PDAX;

(v) Establish, exercise, or defend PDAX’s legal claims;

(vi) Fulfill any other purposes directly related to the above-stated purposes.

g. Geographic Location of the Processing – The Personal Data shall be processed by PDAX at the geographic location specified in DOD.

PDAX shall, at least thirty (30) days prior to effecting any change in the geographic location, notify the User in writing of such intended change and provide reasonable proof that such change shall not adversely affect the TPOSM currently in place or impact the privacy rights of the Data Subjects.

h. Obligations of User – Pursuant to the requirements of the DPA, the User hereby undertakes to:

(i) Secure the written consent of each Data Subject;

(ii) Process personal data to the extent allowed by the Data Subject in accordance with this Addendum, PDAX Terms and Conditions, Privacy Policy, all applicable PDAX Platform Rules and Applicable Laws and Rules;;

(iii) Specify the persons and/or entities authorized to receive, access, process, and/or transmit the information obtained and processed by PDAX, giving PDAX the right to refuse to give information to persons or entities not designated by User.

i. Obligations of PDAX – Pursuant to the requirements of the DPA, PDAX hereby undertakes to:

(i) Process Personal Data only upon the documented instructions of User, including transfers of personal data to another country or an international organization, to the extent contemplated under the DOD, unless such transfer is authorized or required by Applicable Laws and Rules;

(ii) Ensure that an obligation of confidentiality is imposed on persons authorized by PDAX pursuant to this Sub-Agreement to process the Personal Data;

(iii) Implement appropriate security measures and comply with the DPA;

(iv) Assist the Personal Information Controller, by appropriate TPOSM and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights;

(v) Make available to the User all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections to the extent required by Applicable Laws and Rules and within reasonable office hours with prior written notice to PDAX;

(vi) Immediately inform the User if, in its opinion, an instruction infringes the DPA;

(vii) Assist User, as may be practicable and necessary, in ensuring compliance with the DPA, taking into account the nature of processing and the information available to PDAX;

(viii) At the choice of the User, delete or return all Personal Data to the User upon termination of, and subject to, the Terms and Conditions, Privacy Policy, the Addendum and this Sub-Agreement; and

(ix) to the extent relevant to the User, report all available information to the User within forty-eight (48) hours from knowledge of, or reasonable belief that, a personal data breach or a security incident involving Personal Data of a User's Client or any Personal Data disclosed by the User to PDAX has occurred, and extend full cooperation to the User to enable the User to comply with its obligations under the DPA or Applicable Laws and Rules.

j. **Security Obligations of PDAX** – Pursuant to its obligation to maintain the appropriate TPOSM, PDAX warrants that, at minimum, it shall have the following security measures:

Organizational Security Measures

(i) That it has a designated individual who functions as Data Protection Officer.

(ii) That it has implemented appropriate data protection policies that provide for TPOSM, taking into account the nature, scope, context, and purposes of the processing, as well as the risks posed to the rights and freedoms of Data Subjects.

- The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
- The policies shall implement appropriate security measures that, by default, ensure only Personal Data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of Personal Data collected, including the extent of processing involved, the period of their storage, and their accessibility.

- The policies shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.

(iii) That it shall maintain records that sufficiently describe its data processing system and identify the duties and responsibilities of those individuals who will have access to Personal Data. Records shall include:

- Information about the purpose of the processing of Personal Data, including any intended future processing or data sharing;
- A description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the processing;
- General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of Personal Data;
- A general description of the TPOSM in place; and
- The name and contact details of each Party, its representatives, the sub-Users (if applicable), and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

(iv) That its employees shall operate and hold Personal Data under strict confidentiality. This obligation shall continue even upon termination of the employee’s employment.

Physical Security Measures

(i) That it has implemented policies and procedures to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;

(ii) That the design of its office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

(iii) That the duties, responsibilities and schedule of individuals involved in the processing of personal data are clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time;

(iv) That it has implemented policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of Personal Data; and

(v) That it has implemented policies and procedures that prevent the mechanical destruction of files and equipment. The room and workstation used in the processing of Personal Data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Technical Security Measures

(i) That it has implemented safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

(ii) That it has the ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

(iii) That it performs regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a Personal Data Breach;

(iv) That it has the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(v) That it has a process for regularly testing, assessing, and evaluating the effectiveness of security measures; and

(vi) That it encrypts Personal Data during storage and while in transit, authentication process, and it has implemented other technical security measures that control and limit access.

k. **Indemnification** – User agrees to irrevocably, unconditionally, and fully indemnify and hold PDAX or the PDAX Group free and harmless from and against any and all claims, suits, actions or demands or losses, damages, costs and expenses including, without limiting the generality of the foregoing, attorney's fees and costs of suit that User may face, suffer or incur by reason or in respect of:

(i) User's or the User's Client's breach of any of the warranties and obligations set forth in the Addendum, PDAX Terms and Conditions, Privacy Policy, all applicable PDAX Platform Rules and this Sub-Agreement, regardless of the cause of such breach; or

(ii) Any act, omission or negligence of the User or the User's Clients that causes or results in the breach by PDAX of its obligations under the DPA and Applicable Laws and Rules.

l. **Data Subject Rights** – Each Party shall respect the following rights accorded to Data Subjects by the DPA:

(iii) *Right to be informed*. Data Subjects have the right to be informed whether Personal Data pertaining to them shall be, are being, or have been processed, including the existence of automated decision-making and profiling. This Sub-Agreement may be accessed by the Data Subject upon written request submitted to any of the Parties.

(iv) *Right to object.* Data Subjects have the right to object to the processing of their Personal Data, including processing for direct marketing, automated processing or profiling. They may withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the Data Subject.

(v) *Right to access.* Data Subjects have the right to request access to any of their Personal Data, subject to certain restrictions.

(vi) *Right to rectification.* Data Subjects have the right to dispute the inaccuracy or error in the Personal Data and have the PIC correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.

(vii) *Right to erasure or blocking.* Data Subjects have the right to suspend, withdraw or order the blocking, removal or destruction of his or her Personal Data from the PIC's filing system.

(viii) *Right to damages.* Data Subjects have the right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data, taking into account any violation of the rights and freedoms of the Data Subject.

(ix) Right to lodge a complaint with the National Privacy Commission.

m. **Communications Regarding Data Privacy Concerns** – For questions, requests, and notifications, communication may be directed to each Party's designated Data Protection Officer or his/her replacement or substitute.

n. **Notarized Data Outsourcing Agreement** - To the extent required by Applicable Laws and Rules, the Parties may be required to execute a notarized Data Outsourcing Agreement.