DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") is entered into by and between Hodlnaut a Singapore based corporation with offices at 24 Raffles Place Clifford Centre, Singapore (048621) (the "**Customer**") and Glykka LLC, a company incorporated under the laws of the United States of America and having its registered office at 750 N Saint Paul St Ste 250, PMB 42273 Dallas, Texas 75201-3206 US. ("**the Company**").

The Customer and the Company are hereinafter referred to individually as a "**Party**" and collectively as the "**Parties**")

This DPA forms an integral part of the Terms of Service available at https://signeasy.com/terms (the "**Terms**") and is applicable where the Company Processes the Customer's Personal Data originating from the European Economic Area ("**EEA**") and/or Switzerland.

1. Definitions

Terms not specifically defined herein shall have the meaning ascribed thereto in the Terms.

In this DPA, the following terms shall have the following meanings:

"**Data Protection Laws**" shall mean the data protection laws of the country in which the Customer is established, including laws and regulations of the, European Union, the EEA and their member states and Switzerland, including, the GDPR and any applicable national laws made under it where Customer is established in the EEA; and the Swiss Federal Act on Data Protection (as may be amended or superseded) where Customer is established in Switzerland.

"**GDPR**" shall mean the 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Data**" shall mean any information relating to an identified or identifiable natural person as defined by the GDPR that is Processed by the Company as part of providing the service(s) to the Customer.

"**SCCs**" means the standard contractual clauses as approved by the European Commission (Implementing Decision (EU) 2021/914 of 04 June 2021) and available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en (as amended or updated from time to time). For the avoidance of doubt, Modules 2 and 3 of the SCCs shall apply as set out in Clause 12.

"**Sensitive Personal Information**" means information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also includes information about an individual's criminal offences or convictions, as well as any other information deemed sensitive under applicable data protection laws

"**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Processor**" and "**Process**" shall have the meaning given to them in the GDPR.

2. Scope and Responsibilities

2.1 This DPA applies to Processing of Personal Data forming a part of the Customer Data, originating from the EEA and/or Switzerland.

2.2 The Company shall Process Personal Data only on the Customer's behalf and at all times only in accordance with this DPA. For the avoidance of doubt, the Parties acknowledge that the Customer may be either the Controller or the Processor of the Personal Data. Where Customer is the Controller, The Company is the Processor and where Customer is a Processor, The Company acknowledges that it will be a sub-processor to the Customer.

2.3 Within the scope of the Terms, each party shall be responsible for complying with its respective obligations as Controller and Processor under Data Protection Laws.

3. Term and Termination

3.1 This DPA becomes effective upon the Customer subscribing to the service(s) by agreeing to the Terms. It shall continue to be in full force and effect as long as the Company is Processing Personal Data pursuant to the Terms and shall terminate automatically thereafter.

3.2 Where amendments are required to ensure compliance of this DPA with Data Protection Laws, the Parties shall make reasonable efforts to agree on such amendments upon the Customer's request. Where the Parties are unable to agree upon such amendments, either party may terminate the Terms in accordance with the termination procedure contained therein.

4. Processing Instructions

4.1 The Company will Process Personal Data in accordance with the Customer's instructions. This DPA contains the Customer's initial instructions to the Company. The Parties agree that the Customer may communicate any change in its initial instructions to the Company by way of amendment to this DPA, which shall be signed by the Parties.

4.2 For the avoidance of doubt, any instructions that would lead to Processing outside the scope of this DPA (e.g., because a new Processing purpose is introduced) will require a prior agreement between the Parties and, where applicable, shall be subject to the contract change procedure under the respective agreement.

4.3 The Company shall, without undue delay, inform the Customer in writing if, in its opinion, an instruction infringes Data Protection Laws, and provide a detailed explanation of the reasons for its opinion in writing.

5. The Company Personnel

The Company will restrict its personnel from Processing Personal Data without authorization. The Company will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

6. Disclosure to Third Parties; Data Subjects Rights

6.1 The Company will not disclose Personal Data to third parties except: (i) to employees, service providers, or advisers who have a need to know the Personal Data and are under confidentiality obligations at least as restrictive as those described under this DPA or (ii) as required to comply with valid legal process in accordance with the terms of the Agreement.

6.2 The Company will not disclose Personal Data to any government agency, court, or law enforcement except with the Customer's written consent or as necessary to comply with applicable mandatory laws. If the Company is obliged to disclose Personal Data to a law enforcement agency, then the Company agrees to give the Customer reasonable notice of the access request prior to granting such access, to allow the Customer to seek a protective order or other appropriate remedy. If such notice is legally prohibited, then the Company will take reasonable measures to protect the Personal Data from undue disclosure as if it were the Company's own confidential information being requested and shall inform the Customer promptly as soon as possible if and when such legal prohibition ceases to apply.

6.3 In case the Customer receives any request or communication from Data Subjects which relates to the Processing of Personal Data ("**Request**"), the Company shall reasonably provide the Customer with full cooperation, information and assistance ("**Assistance**") in relation to any such Request where instructed by the Customer.

6.4 Where the Company receives a Request, it shall (i) not directly respond to such Request, (ii) forward the Request to the Customer within five (**5**) business days of identifying the Request as being related to the Customer and (iii) provide Assistance according to further instructions from the Customer.

7. Technical and Organizational Measures

7.1 The Company shall implement and maintain appropriate technical and organizational security measures to ensure that Personal Data is Processed according to this DPA, to provide assistance and to protect Personal Data against a Personal Data Breach ("**TOMs**") as specified in Schedule B hereto.

8. Assistance with Data Protection Impact Assessment

8.1 Where a Data Protection Impact Assessment ("**DPIA**") is required under applicable Data Protection Laws for the Processing of Personal Data, the Company shall provide, upon request, to the Customer any information and assistance reasonably required for the DPIA including assistance for any communication with data protection authorities, where required, unless the requested information or assistance is not pertaining to the Company's obligations under this DPA.

8.2 We will provide reasonable assistance and information to You in fulfilling any legal obligations that You may have under the GDPR regarding data protection impact assessments, data and systems inventory, records of Processing, and related consultations of data protection authorities, or in the event of an investigation by any governmental authorities, if and to the extent that such investigation relates to Personal Data Processed by Us in accordance with the Agreement. Such assistance will be at Your sole expense, except where such an investigation was required due to Our failure to act in accordance with the Agreement.

8.3 The Customer shall pay the Company reasonable charges for providing the assistance in clause 8, to the extent that such assistance cannot be reasonably accommodated within the normal provision of the services.

9. Information Rights and Audit

9.1 The Company shall, in accordance with Data Protection Laws, make available to the Customer on request in a timely manner such information as is necessary to demonstrate compliance by the Company with its obligations under the Data Protection Laws.

9.2 The Company shall, upon reasonable notice, allow for and contribute to audits of its Processing of Personal Data, as well as the TOMs (including data Processing systems, policies, procedures and records), during regular business hours and with minimal interruption to the Company's business operations. Such audits shall be conducted by the Customer, the Customer's affiliates or an independent third party on the Customer's behalf (which will not be a competitor of the Company's business) that is subject to reasonable confidentiality obligations.

9.3 The Customer shall pay the Company reasonable costs of allowing or contributing to audits or inspections in accordance with clause 9.2 where the Customer wishes to conduct more than one audit or inspection every twelve (12) months.

9.4 The Company will immediately refer to the Customer any requests received from national data protection authorities that relate to its Processing of Personal Data.

9.5 The Company undertakes to reasonably cooperate with the Customer in its dealings with national data protection authorities and with any audit requests received from national data protection authorities.

10. Personal Data Breach Notification

In respect of any Personal Data Breach (actual or reasonably suspected), the Company shall:

10.1 notify the Customer of a Personal Data Breach involving the Company or a sub-processor without undue delay and it shall be the Customer's responsibility to inform the supervisory authority of such breach within seventy-two (72) hours of notice by the Company;

10.2 provide reasonable information, cooperation and assistance to the Customer in relation to any action to be taken in response to a Personal Data Breach under Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and national data protection authorities.

11. Use of sub-processors

11.1 The Company has the Customer's general authorisation for the engagement of sub-processors from an agreed list. The Company shall specifically inform in writing the Customer of any intended changes of that list through the addition or replacement of sub-processors at least fifteen (15) days in advance, thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s), provided such objection is based on reasonable grounds relating to data protection. In such an event, the Company will either not appoint or replace the sub-processor or, if this is not possible, either Party may terminate the service(s) (without prejudice to any fees incurred by the Customer prior to such suspension or termination). The

Company shall provide the Customer with the information necessary to enable the Customer to exercise the right to object.

11.2 Where the Company engages a sub-processor for carrying out specific processing activities (on behalf of the Customer), 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 Company under this DPA and in accordance with Art. 28 of the GDPR. The Company shall ensure that the sub-processor complies with the obligations to which the Company is subject to under this DPA and the GDPR.

11.3 The Company shall remain fully responsible to the Customer for the performance of the sub-processor's obligations in accordance with its contract with the Company.

12. International Data Transfers

12.1 The Company shall at all times provide an adequate level of protection for the Personal Data, wherever processed, in accordance with the requirements of Data Protection Laws To the extent that the Company Processes any Personal Data originating from EEA, and/or Switzerland (in a country that has not been designated by the European Commission as providing an adequate level of protection for Personal Data), the SCCs, which are incorporated by reference, shall apply to any such Processing as follows:

a. Module 2 (Controller to Processor) shall apply where the Customer is a Controller and the Company is a Processor
b. Module 3 (Processor to Processor) shall apply where the Customer is a Processor and the Company is a sub-processor

12.2 Purely for the purposes of descriptions in the SCCs and only as between the Parties, the Customer agrees that it is the "data exporter" and the Company is the "data importer" under the SCCs (notwithstanding that the Customer may be located outside the EEA and/or Switzerland and may be a Processor acting on behalf of third-party Controllers). Further, Schedules A, B and C of this DPA will take the place of Annexes I, II and III of the SCCs respectively.

12.3 For the purposes of Clause 17 of the SCCs, the governing law of the SCCs shall be the law of the country that the operations are based in. For the purposes of Clause 18 of the SCCs, any dispute arising from the SCCs shall be resolved by the courts of the country of operations/ Switzerland.

13. Deletion or Return of Personal Data

The Company shall delete all Content, including Personal Data within thirty (30) days from the date of termination of the Customer's account. Prior to termination or expiration of the Agreement for any reason, You may retrieve Personal Data processed by Us in accordance with the terms of the Agreement, and at Customer's request provided in writing to Us We will promptly return or delete Personal Data from Signeasy platform, unless applicable law requires the storage of the Personal Data. This requirement shall not apply to the extent that the Company is permitted by applicable law to retain some or all of the Personal Data, in which event the Company shall isolate and protect the Personal Data from any further processing.

14. Customer Responsibilities

Customer acknowledges that it is responsible for properly implementing access and use controls and configuring certain features and functionalities of Signeasy that Customer may elect to use and that it will do so in such manner that Customer deems adequate to maintain appropriate security, protection, deletion, and backup of Personal Data. We will be entitled to rely solely on Customer or Customer Affiliate's instructions relating to Personal Data Processed by Us. You are responsible for coordinating all communication with Us under this DPA, including, without limitation, any communication in relation to this DPA on behalf of its Affiliates.

15. Miscellaneous

15.1 In case of any conflict, the provisions of this DPA shall take precedence over the Terms or provisions of any other agreement with the Parties. In case of any conflict between this DPA and the SCCs, the SCCs shall take precedence over the provisions of the rest of the DPA.

15.2 No Party shall receive any remuneration for performing its obligations under this DPA except as explicitly set out herein or in another agreement.

15.3 Where this DPA requires a "written notice" such notice can also be communicated per email to the other party.

15.4 Any supplementary agreements or amendments to this DPA must be made in writing and signed by both Parties.

15.5 Should individual provisions of this DPA become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this DPA.

GLYKKA LLC	CUSTOMER
Name: Sunil Patro Designation: CEO Date: 03/01/22	Name: Shayna Ang Designation: HR, EA to CEO Date: 04/01/22

SCHEDULE A

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: Hodlnaut

   Address: 24 Raffles Place Clifford Centre, Singapore (048621)

   Contact person's name, position and contact details: Shayna Ang, HR and EA to CEO; shayna@hodlnaut.com

   Activities relevant to the data transferred under these Clauses: https://signeasy.com/terms https://signeasy.com/privacy

   Signature and date: Shayna Ang 04/01/22

   Role(controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: Glykka LLC

   Address: 750 N Saint Paul St Ste 250, PMB 42273 Dallas, Texas 75201-3206 US

   Contact person's name, position and contact details: Bineeta Mitra, Lead - Information Security and Compliances, compliances@signeasy.com

   Activities relevant to the data transferred under these Clauses: https://signeasy.com/privacy ; https://signeasy.com/terms

   Signature and date: 04/01/22

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners, customers or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by the data importer.

Categories of personal data transferred

The transferred Personal Data concerns the following categories of data:

The data exporter determines the categories of Personal Data which could be transferred per the services as stated in the Terms of Service. Such categories may include the following categories of data: name, phone numbers, e-mail address, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data transferred by authorized personnel and may include financial data such as bank account data, credit or debit card data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data transferred. The data exporter shall not disclose (and shall not permit any individual to disclose) any Sensitive Personal Information to the data importer for processing.

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

Personal Data is transferred on a continuous basis

Nature of the processing

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 of data (whether or not by automated means).

Purpose(s) of the data transfer and further processing

Personal Data is transferred in the course of access and use by the data exporter of the services so that the data importer may provide, support, maintain and improve the services.

The data importer may further transfer Personal Data to third-party service providers that host and maintain the data importer's applications, backup, storage, payment processing, analytics and other services as specified in the section on sub-processors below. These third-party service providers may have access to or Process Personal Data for the purpose of providing these services to the data importer.

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

Upon termination of the data exporter's account, the data importer will delete all Personal Data in accordance with clause 13 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

In respect of the SCCs:

Module 2: Transfer Controller to Processor

Module 3: Transfer Processor to Processor

Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the SCCs.

SCHEDULE B

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms and need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.
Measures of encryption of personal data
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Measures for user identification and authorisation
Measures for the protection of data during transmission
Measures for the protection of data during storage
Measures for ensuring physical security of locations at which personal data are processed
Measures for ensuring events logging
Measures for ensuring system configuration, including default configuration
Measures for internal IT and IT security governance and management
Measures for certification/assurance of processes and products
Measures for ensuring data minimisation
Measures for ensuring data quality
Measures for ensuring limited data retention
Measures for ensuring accountability
Measures for allowing data portability and ensuring erasure]
For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter