This Data Protection Addendum (U.S., UK and EU) (the "**Addendum**") is incorporated into and forms part of the agreement you have entered into with our applicable group entity identified in the table below ("**we**", "**us**", and "**our**") (each a "**party**", and together the "**parties**") (the "**Agreement**"). In the event of any conflict between this Addendum and the other provisions of the Agreement or the Privacy Policy, this Addendum will prevail.

The following table sets out the different entities to which this Addendum applies, as well as their relevant role under each applicable Agreement:

	Us			
No	**Party**	**Agreement**	**Delivery**	**Role**
1	System Pay Services Solutions (Malta) Limited ("**SPS Malta**")	Master Services Agreement including Service Schedules 1, 2 and 3 (for 3, see row 2) and 4 (if the Embedded Schedule applies to you, in which case see row 4)	Provision of the Services plus the access to the Partner Services (see row 2), including processing the Protected Data of your third party	SPS Malta is the Controller OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law
2	System Pay Services Limited ("**SPS UK**")	UK E-Money Account Terms, being Service Schedule 3 to the Master Services Agreement (*to the extent you sign the Master Services Agreement referred to in row 1)*	Provision of the Services, including processing the Protected Data of your third party	SPS UK is the controller for the provision of the Services OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law AND SPS Malta is the processor of SPS UK
3	System Pay Services Solutions (US), Inc ("**SPS US**")	Master Services Agreement including Schedules 1, 2 and 3 (if the Embedded Schedule applies to you, in which case see row 4) OR Services Agreement and Payment Service Terms	Provision of the Services, including processing the Protected Data of your third party	SPS US is the Controller OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law

			Provision of the Partner Services (where the Service Partner provides a direct service to you)	SPS US acts as the processor of our Service Partner, who is the controller OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law
		Embedded Schedule (if applicable) OR Embedded Service Terms (if applicable)	We exercise and perform our contractual rights and obligations under the Embedded Services Terms	We are the Controller OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law
			Provision of the Partner Services (where the Service Partner provides a direct service to End-Users)	We are acting as the processor of our Service Partner, who is the controller OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law
You				
No.	**Entity**	**Agreement**	**Delivery**	**Role**
4	You	Master Services Agreement OR Services Agreement and Payment Service Terms	Your exercise and performance of your other contractual rights and obligations	You are the Controller OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law
		Embedded Schedule (if applicable) OR	Provision of Technology and Other Services	You are our processor and a sub-processor to our partners. Your

		Embedded Service Terms (if applicable)		subcontractors will be our Sub-Processors if they support you in delivering the Technology and Other Services OR joint controller or processor, only when so determined by a Supervisory Authority or a court of law

1. Definitions and Interpretation

1.1. Unless the context otherwise requires, capitalised terms used in this Addendum shall have the meaning given to them below, or as otherwise defined in the Agreement:

"**Agreement"** incorporates this	means the agreement between the entity in the table above and you, which Addendum by reference;
"Applicable Laws"	means any laws, regulations, regulatory constraints, obligations or rules in the United Kingdom, Spain, the United States, Singapore or any other relevant jurisdiction, which are applicable to the relevant Agreement and this Addendum (including binding codes of conduct and binding statements of principle incorporated and contained in such rules from time to time), interpreted (where relevant) in accordance with any guidance, code of conduct or similar document published by a relevant regulatory authority;
"Appropriate Safeguards"	means such legally enforceable mechanism(s) for transfers of personal data as may be permitted under the GDPR from time to time, including those set out in Article 46 GDPR, the UK GDPR and the implementation of binding corporate rules pursuant to Article 47 GDPR;
"Controller Data"	has the meaning given to it in Part 3 of this Addendum;
"Data Complaint"	means any formal complaint relating to either party's obligations under the Data Protection Laws relevant to the Agreement, including any complaint by a data subject or any notice, investigation or other action by a Supervisory Authority;
"Data Processing Term"	has the meaning given to it in Schedule 1 of this Addendum;
"Data Protection Laws"	means all applicable data protection laws (and in each case any re-enactment or amendment) in any jurisdiction where we operate (to the extent applicable to the services we provide to you under the relevant Agreement) or in any jurisdiction where you operate (to the extent applicable to the Technology and Other Services you provide under the relevant Agreement), including but not limited to, the Data Protection Act 2018, the UK GDPR, the EU GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Spanish Data Protection Act (Organic Law 3/2018), the U.S. Gramm-Leach-Bliley Act, as well as the applicable state privacy laws, such as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act ("**CCPA**"), and state privacy laws requiring notice of breaches of personal data, the Singapore Personal Data Protection

	Act 2012 and any other directly applicable local or national regulation (or directive) relating to privacy;
"Data Subject Request"	means a request made by a data subject to exercise any rights of data subjects under the Data Protection Laws in connection with the Protected Data;
"Effective Date"	means the effective date of the Agreement;
"Joint Data"	has the meaning given to it in Part 2 of this Addendum;
"Permitted Purposes"	has the meaning given to it in paragraph 1.3 of Part 1 of this Addendum;
"Personal Data Breach"	means a personal data breach in relation to, involving or affecting the Protected Data;
"Processing Instructions"	has the meaning given to it in paragraph 1.1.1 of Part 4 of this Addendum;
"Protected Data"	means any personal data captured in the descriptions in table above in connection
with the	Agreement, in any form or medium, whether collected, generated, received or
otherwise	made available at any time that is processed by any party in its capacity as a joint or independent controller or as a processor in connection with the performance of our obligations under the Agreement;
"Records"	has the meaning given to it in paragraph 5.1 of Part 1 of this Addendum;
"Services"	means those services provided from time to time under and pursuant to the terms of the relevant Agreement;
"Sub-Processor"	means another processor engaged by us or you (when either party is acting as a processor) for carrying out processing activities in respect of the Protected Data under or in connection with the Agreement;
"Supervisory Authority"	means any local, national, or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board, or other body responsible for administering the Data Protection Laws, including the Information Commissioner's Office in the United Kingdom, the Spanish Data Protection Agency in Spain, the Information and Data Protection Commissioner in Malta, and the Personal Data Protection Commission in Singapore; and
"Technology and Other Services"	means those services you provide to us in relation to the Embedded Services Terms of the Agreement;

1.2. Terms, acronyms, phrases and abbreviations utilised in the financial services industry or other pertinent business context will be interpreted in accordance with their generally understood meaning in such industry or business context and lowercase terms used but not defined in this Addendum such as "personal data", "processing", "processor", "controller", "independent controller", "joint controller", "data subject", "organisation", and "data intermediary" have the meanings set out in the Data Protection Laws.

1.3. This Addendum is divided into the following parts:

1.3.1. **Part 1 General Terms** – these terms apply irrespective of the role of the parties;

1.3.2. **Part 2 Joint Controller Terms** – these terms apply only where the parties act as joint controllers;

1.3.3. **Part 3 Controller Terms** – these terms apply where a party acts as an independent controller; and

1.3.4. **Part 4 Processor Terms** – these terms apply where a party acts as a processor.

1.4. If there is any conflict between this Addendum and the Agreement, this Addendum will prevail.

1.5. If there is any conflict between (i) the provisions in Part 1 – General Terms; and (ii) the provisions in any of Part 2 – Joint Controller Terms, Part 3 – Controller Terms, or Part 4 – Processor Terms, the provisions in Part 2 – Joint Controller Terms, Part 3 – Controller Terms, or Part 4 – Processor Terms (as applicable) will prevail.

1.6. We reserve the right to update this Addendum from time to time in accordance with the terms of the Agreement including to comply with our obligations under the Data Protection Laws, to address any changes to the Services or Technology and Other Services including any new functionality or features and/or to cover any additional services that

we may provide to you or you may provide to us, if applicable, from time to time. The prevailing terms of the most recent version of this Addendum made available on our website, and notice will be deemed to be given on the date of publication on our website.

Part 1 – General Terms

1. Scope And Purpose

1.1. This Addendum sets out the principles and procedures that each party shall adhere to and the additional terms, requirements and conditions on which each party will process the Protected Data. When providing the Services to you and when you provide the Technology and Other Services, if applicable, and otherwise exercise and perform rights and obligations under the Agreement, each party may act as a joint controller, independent controller, or processor of Protected Data.

1.2. Nothing in this Addendum reduces or replaces the parties' obligations under the Data Protection Laws in relation to the protection of personal data.

1.3. Subject to paragraph 1.4 of this Part 1, the parties agree to only process the Protected Data for the provision of the Services or Technology and Other Services, or in contemplation of the provision of the Services by us or the Technology and Other Services by you, for the performance and exercise of each party's rights and obligations under the Agreement, for each party's legitimate business purposes (including compliance with its legal and regulatory obligations, IT security and administration purposes) or for any other purposes set out in Schedule 1 to this Addendum (as applicable) ("Permitted Purposes") and shall not process the Protected Data in a way that is incompatible with the Permitted Purposes.

1.4. Each party shall process the Protected Data in compliance with:

1.4.1. the Data Protection Laws; and

1.4.2. the terms of this Addendum.

1.5. Any queries relating to this Addendum and/or the processing of personal data by either party should be sent to:
Us - Our Data Protection Officer, who may be contacted at dpo@bvnk.com.
Embedded Partner (if applicable) - see details in the Commercial Terms annexed to the Agreement.

2. Technical and Organisational Measures

2.1. Each Party shall only provide the Protected Data to another third party by using secure methods as set out in Schedule 2 to this Addendum.

2.2. Each Party shall implement and maintain appropriate technical and organisational measures to:

2.2.1. ensure that the processing of the Protected Data will meet the requirements of the Data Protection Laws and ensure the protection of the rights of data subjects; and

2.2.2. ensure that the processing and storage of the Protected Data maintains the highest standards of accessibility, availability, integrity, authenticity, and confidentiality.

2.2.3. ensure the security, integrity, availability, and confidentiality of the Protected Data and protect against unauthorised or unlawful processing of the Protected Data, accidental loss or destruction of, or damage to Protected Data such measures to be appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected.

2.3. The level of technical and organisational measures as at the Effective Date, having regard to the matters referred to in

paragraph 2.2 of this Part 1, is as set out in Schedule 2 to this Addendum. The measures shall be regularly tested, assessed, and evaluated to assess their effectiveness in ensuring the security of the processing, and each party shall maintain records of such testing. Each party shall keep the measures under review and shall carry out such updates as each party deems appropriate throughout the Data Processing Term.

2.4. Each party will ensure that its personnel involved in the processing of Protected Data are appropriately trained to handle and process the Protected Data in accordance with the technical and organisational security measures set out in Schedule 2 to this Addendum, together with any applicable Data Protection Laws and guidance from a relevant Supervisory Authority.

2.5. The level, content and regularity of training referred to in paragraph 2.4 shall be proportionate to the personnel's role, responsibility, and frequency with respect to their handling and processing of the Protected Data.

2.6. Each Party's Personnel shall be subject to written confidentiality obligations which cover their processing of any Protected Data.

3. International Data Transfers

3.1. **International data transfers between us**. To the extent use of the Services or Technology and Other Services requires, under the Data Protection Laws, an onward transfer mechanism for either party to lawfully transfer Protected Data from a jurisdiction such as the EEA or the United Kingdom or any such other jurisdiction where either party operates to the other jurisdiction (if that party is located outside of the UK and the EEA and it is required to have Appropriate Safeguards in place) ("**Transfer Mechanism**"), the terms outlined in Schedule 3 (Cross Border Transfer Mechanisms) of this Addendum will apply.

3.2. **International data transfers to other third parties**. The parties will not transfer, access or process Protected Data outside of the UK and the EEA, including to a Sub-Processor located in such a country or territory, unless:

3.2.1. there is a European Union finding of adequacy in respect of that country or territory pursuant to Article 45 GDPR or as otherwise provided under the Data Protection Laws;

3.2.2. the relevant party has ensured that any such transfer complies with the Data Protection Laws by having in place Appropriate Safeguards, and the party has taken steps to satisfy itself that:

3.2.2.1. the level of protection afforded to the Protected Data in the destination country or territory is equivalent to the level of protection that would be afforded to Protected Data in the UK or EEA;

3.2.2.2. any data importer shall provide the other party with relevant sources and information relating to the destination country or territory and the laws applicable to the transfer in that destination country in order to substantiate the matters set out in 3.2.2.1 above; and

3.2.2.3. any data importer is contractually obliged to keep the other party informed of any development affecting or likely to affect the level of protection the transferred Protected Data receives in the importer's country; or

3.2.3. the relevant party is otherwise permitted to do so by virtue of a derogation in Article 49 of the GDPR or as otherwise provided under the Data Protection Laws.

3.3. If, for whatever reason, the transfer of Protected Data pursuant to paragraphs 3.2.1, 3.2.2 or 3.2.3 of this Part 1 – General Terms ceases to be lawful, the party will immediately implement other Appropriate Safeguards and ensure that the level of protection afforded to the Protected Data in the destination country or territory is equivalent to the level of

protection that would be afforded to Protected Data in the EEA and/or in the United Kingdom. Where a party cannot do that, the party will cease any such transfer of Protected Data unless the other party expressly authorises the transfer to continue.

4. Using Processors

4.1. Where a party engages a processor or Sub-Processor to carry out any processing activities in respect of Protected Data, the party will:

4.1.1. ensure that there is a written contract in place with each processor or Sub-Processor which requires the processor or Sub-Processor to only carry out such processing as may be necessary from time to time for the purposes of its engagement by us in connection with the Agreement and to comply with terms and conditions which offer materially the same level of protection for the Protected Data as those set out in this Part 1 – General Term;

4.1.2. be responsible for the acts and omissions of any processor or Sub-Processor in the performance of its data processing obligations under the Agreement as if they were our own acts and omissions.

4.2. Each party will ensure that all persons authorised by us (or by any processor or Sub-Processor) to process Protected Data are subject to an obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case each party will, where practicable and not prohibited by Applicable Law, notify the other party of any such requirement before such disclosure).

5. Records

5.1. Each Party will maintain complete, accurate and up-to-date written records of all categories of processing activities carried out in accordance with the Data Protection Laws (the "**Records**") and notify the other party of any change to the location of processing and/or sub-processing.

6. Reporting and General Obligations

6.1. Each Party will comply with its obligations under the Data Protection Laws to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) to the data subjects.

6.2. Each party agrees to notify the other party promptly (and in any event within 48 (forty-eight) hours if a party becomes aware of a Personal Data Breach by that party or otherwise in connection with the Services or Technology and Other Services and provides the other party with full details of the Personal Data Breach. Each party will provide reasonable co-operation and assistance to the other party as is necessary to facilitate the handling of a Personal Data Breach in an expeditious and compliant manner and to enable the other party to comply with its obligations under the Data Protection Laws. Each party will not release or publish any filing, communication, notice, press release or report concerning any Personal Data Breach by it or otherwise in connection with the Services or Technology and Other Services unless required to do so under the Data Protection Laws and/or by a Supervisory Authority, in which case, it will notify the other party in advance of such requirement.

6.3. Each party will take prompt action to investigate any Personal Data Breach involving Protected Data and to identify, prevent and mitigate the effects of and to remedy any such Personal Data Breach.

6.4. Each party will act reasonably to keep the other party informed of ongoing developments in relation to any Personal Data Breach.

7. Parties' Obligations

7.1. Irrespective of whether a party acts as a controller, joint controller, or processor:

7.1.1. each party is solely responsible for making an independent determination as to whether the technical and organisational measures implemented by the other party are adequate and meet the requirements of the Data Protection Laws and any other obligations you have under Applicable Laws;

7.1.2. each party will comply, at all times, with its obligations as a controller (as applicable) and will provide your services to clients in compliance with the Data Protection Laws;

7.1.3. each party will maintain any valid registrations and pay any fees as required by your Supervisory Authority to cover its processing activities, including those contemplated under the Agreement;

7.1.4. each party will maintain adequate data processing, privacy and IT security policies in relation to your processing of personal data and any cybersecurity incident that meet the requirements of Data Protection Laws. Each party will comply with and procure that its personnel comply at all times with such policies. Each party will ensure that its personnel are subject to written confidentiality obligations which cover their processing of personal data.;

7.1.5. each party will provide all necessary, fair and transparent information and notices to, and obtain all necessary consents from, any data subjects whose Protected Data are processed pursuant to this Addendum (including any personnel, any third parties and customers), so that the other party is lawfully able to use or otherwise process this Protected Data for the Permitted Purpose pursuant to this Addendum without needing any further consent, approval or authorisation and upon our request from time to time. Each party will ensure that such information and notices detail the purposes of processing of Protected Data as required for the Permitted Purpose, the legal basis for such processing, the recipients of the Protected Data and such other information as required to be given by a controller to data subjects under the Data Protection Laws;

7.1.6. if requested by the other party, each party will promptly provide reasonable evidence that it has provided all necessary information and notices to and obtained all necessary consents from data subjects and otherwise complied with Clause 7.1.5;

7.1.7. each party may assume that any disclosure or transfer of personal data to it by the other party (directly or indirectly) is done so in a manner which is compliant with the Data Protection Laws;

7.1.8. each party will ensure that any personal data you disclose or otherwise transfer to the other party is accurate;; and

7.1.9. each party will not disclose or transfer to the other any excessive or irrelevant personal data. Each party will delete any excessive or irrelevant personal data;

7.1.10. each party will notify the other party promptly (and in any event within 48 (forty-eight) hours if it becomes aware of a Personal Data Breach in connection with the Services and will provide the other party with full details of the Personal Data Breach. Each party will provide reasonable co-operation and assistance to the other as is necessary to facilitate the handling of a Personal Data Breach in an expeditious and compliant manner and to enable compliance with the Data Protection Laws. Neither party will release or publish any filing, communication, notice, press release or report concerning any Personal Data Breach or otherwise in connection with the Services unless required to do so under the Data Protection Laws and/or by a Supervisory Authority, in which case, each party will notify the other party in advance of such requirement;

7.1.11. each party will notify the other promptly (where legally permissible and within no more than 2 (two) business days if it receives or becomes aware of a Data Complaint, and will provide reasonable co-operation and assistance as is necessary to deal with such Data Complaint;

7.1.12. each party will provide the other with reasonable cooperation and assistance as may be required from time to time to enable the other its to comply with their obligations under the Data Protection Laws, including those obligations relating to security, Data Subject Requests, data protection impact assessments and consultations with a Supervisory Authority; and

7.1.13. each party will comply with any additional obligations applicable to it in the other Parts of this Addendum.

8. Data Retention

8.1. Neither party will retain Protected Data for longer than is necessary to carry out any Permitted Purpose, unless a longer period is required under Applicable Law.

8.2. Each party will maintain and comply with its data retention policy, details of which each party will provide to the other on written request.

Part 2 – Joint Controller Terms

Where the parties process Protected Data as joint controllers under or otherwise in connection with the Agreement ("**Joint Data**"), the provisions set out in this Part 2 - Joint Controller Terms will apply to the processing of Joint Data by said parties, in addition to Part 1 – General Terms.

1 Processing Joint Data

1.1 Each party will comply with its controller obligations in the Data Protection Laws in connection with its processing of Joint Data.

1.2 Each party agrees that:

1.2.1 for the Joint Data, the parties act together to determine the purpose and means of processing;

1.2.2. it will process the Joint Data solely for the Permitted Purpose and in accordance with Schedule 1 as updated from time to time;

1.2.3 it will ensure that the Joint Data has been collected, processed, and transferred in accordance with the Data Protection Laws as applicable to that Joint Data;

1.2.4 it will be responsible for providing all necessary, fair and transparent information and notices to data subjects and will ensure that such information and notices details the processing of Joint Data as required for the Permitted Purpose, the legal basis for such processing, the recipients of the Joint Data (including the other party, any third parties or a regulator) and such other information as required to be given by a controller to data subjects under the Data Protection Laws. Such information and notices will be transparent as to the arrangement between the parties in compliance with the Data Protection Laws;

1.2.5 it will cooperate with the other party to provide any information reasonably required to enable the other party to produce and publish its information and notices in accordance with paragraph 1.2.4 of this Part 2– Joint Controller Terms;

1.2.6 it will ensure that any data subject who wants to make a Data Subject Request has an easily accessible point of contact to do so; and

1.2.7 it will reasonably assist the other party in ensuring compliance with the other party's obligations under the Data Protection Laws with respect to security, Personal Data Breach notifications, data protection impact assessments and consultations with Supervisory Authorities, insofar as they relate to the processing of Joint Data.

2 Data Subject Requests and Data Complaint Handling

2.1 If a party receives a Data Subject Request and/or a Data Complaint relating to the processing of Joint Data, it will promptly notify the other party (and in any event within 48 (forty-eight) hours of receipt of the Data Subject Request) and comply with the provisions of this paragraph 2.

2.2 As between the parties, responsibility for compliance with and responding to:

2.2.1 any Data Subject Request – falls on the party which first received such Data Subject Request; and

2.2.2 any Data Complaint regarding the processing of Joint Data falls on the party which receives the Data

Complaint,

unless agreed otherwise by the parties.

2.3 The parties will provide reasonable assistance to one another to assist with handling Data Subject Requests and Data Complaints relating to the processing of Joint Data.

2.4 Each party will deal with a Data Subject Request or a Data Complaint relating to the processing of Joint Data in a timely and professional manner and in accordance with the requirements of the Data Protection Laws (including with respect to any timescales). Neither party will respond to a Data Subject Request or Data Complaint relating to the processing of Joint Data, without consultation with the other party, unless such failure to respond would cause it to be in breach of the Data Protection Laws and/or it is requested to respond by a Supervisory Authority.

3 Personal Data Breaches

3.1 If a Personal Data Breach occurs in relation to the Joint Data processed by either party:

3.1.1 the party that discovers the Personal Data Breach will notify the other party without undue delay (and in any event within 48 (forty-eight) hours of becoming aware of the Personal Data Breach), and will provide a detailed description of the Personal Data Breach, including the details of the type of data and the identity of the affected person(s) as soon as such information can be collected or otherwise becomes available, as well as any other information that the other party may reasonably request from time to time;

3.1.2 the parties will reasonably cooperate to determine the cause of the Personal Data Breach and who should notify the Supervisory Authority and/or the data subject(s) if required. In the absence of any agreement, each party will be entitled to notify the Supervisory Authority and/or data subject(s); and

3.1.3 the party suffering the Personal Data Breach will take action immediately to carry out any recovery or other action necessary to remedy the Personal Data Breach.

3.2 If a party becomes aware of a Personal Data Breach in relation to the Joint Data, that party will notify the other party without undue delay. Notifications to us shall be sent to dpo@bvnk.com, and notifications to you shall be sent to the Embedded Partner (if applicable) whose details are set out in the Commercial Terms annexed to the Agreement.

4 Allocation of Responsibility

4.1 The Parties acknowledge that, to the extent they qualify as Joint Controllers for certain Processing operations under Applicable Data Protection Laws, each Party shall be responsible solely for the obligations assigned to it under this Agreement and any Joint Controller Arrangement established between the Parties.

4.2 Except as expressly provided herein, no Party shall be deemed responsible for the other Party's compliance with its respective Controller obligations.

5 Regulatory Cooperation

5.1 Each Party shall provide the other with reasonable cooperation, information, and documentation required to respond to inquiries or investigations from Supervisory Authorities relating to Joint Processing Activities.

5.2 Neither Party shall make any admission, settlement, or voluntary disclosure to a Supervisory Authority relating to Joint

Processing Activities without the other Party's prior written consent, unless legally prohibited or required.

6 Liability Exclusions and Limitations

6.1 To the extent permitted by law, any contractual liability caps applicable under the Agreement shall not apply to:

6.1.1 breaches of confidentiality;

6.1.2 breaches of data protection or information security obligations;

6.1.3 unlawful Processing arising from failure to establish a lawful basis; or

6.1.4 the indemnification obligations set out in this Clause.

6.2 Nothing herein shall limit either Party's liability for fraud, gross negligence, wilful misconduct, or any liability that cannot lawfully be limited.

Part 3 – Controller Terms

Where a party processes Protected Data as an independent controller under or otherwise in connection with the Agreement ("**Controller Data**"), the provisions set out in this Part 3 Controller Terms will apply to the processing of Controller Data by us, in addition to Part 1 – General Terms.

1. Processing Controller Data

1.1 Each party will comply with its controller obligations under the Data Protection Laws in connection with its processing of Controller Data.

1.2 Each party will:

1.2.1 process the Controller Data solely for the Permitted Purpose and in accordance with Schedule 1 to this Addendum as updated from time to time;

1.2.2 provide all necessary, fair and transparent information and notices to data subjects and will ensure that such information and notices detail the processing of Controller as required for the Permitted Purpose, the legal basis for such processing, the recipients of the Controller Data (including third parties or a regulator) and such other information as required to be given by a controller to data subjects under the Data Protection Laws; and

1.2.3 ensure that any data subject who wants to make a Data Subject Request in connection with Controller Data has an easily accessible point of contact to do so.

2. Data Subject Requests

2.1 If a party receives a Data Subject Request and/or a Data Complaint relating to the processing of Controller Data, to the extent legally permissible, it will promptly notify the other party (and in any event within 48 (forty-eight) hours of receipt of the Data Subject Request and/or Data Complaint) and, unless otherwise required under Applicable Law or by a Supervisory Authority, the party, as controller, will be responsible for and will handle such Data Subject Request and/or Data Complaint in compliance with the Data Protection Laws.

Part 4 – Processor Terms

Where a party processes Protected Data on behalf of the other party as a processor, or as a "service provider" for the purposes of the CCPA (the "**Processing Party**"), under or otherwise in connection with the Agreement, the provisions set out in this Part 4 – Processor Terms will apply to the processing of Protected Data, in addition to Part 1 – General Terms.

1. Instructions and Details of Processing

1.1. Insofar as the Processing Party processes Protected Data on behalf of the other party, it shall:

1.1.1. unless required to do otherwise by Applicable Laws, (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Agreement, Schedule 1 to this Addendum and any other documented instructions from the Controller ("**Processing Instructions**"); and

1.1.2. if Applicable Laws require the Processing Party to process Protected Data other than in accordance with the Processing Instructions, notify the other party of any such requirement before processing the Protected Data (unless Applicable Laws prohibit such information on important grounds of public interest).

1.2. Specifically relating to CCPA compliance:

1.2.1. the Processing Party will not combine any Protected Data it receives on behalf of the other party with any personal data the Processing Party receives from other controllers or that the Processing Party receives from interactions with the other party's customers or end-users, unless specifically permitted under the CCPA; and

1.2.2. the Processing Party will promptly notify the other party if unable to meet its data privacy obligations under the Agreement, this Addendum, or Data Protection Laws.

2. Personnel and Other Processors

2.1. The Processing Party may engage a Sub-Processor to carry out any processing activities in respect of the Protected Data d subject to compliance by the party with paragraphs 2.2 and 2.3 of this Part 4, and paragraphs 3 and 5 of Part 1 above.

2.2. The Processing Party will:

2.2.1. provide details to the other party of any Sub-Processor. Any Sub-Processor agreed by the other party as at the Effective Date is set out in the list of the Help Centre or as shared by you with us;

2.2.2. notify the other party 30 days in advance of any change in a Sub-Processor (through the addition or replacement of a Sub-Processor) and shall provide such information as necessary to enable the other party to decide whether to consent to the change. The other party shall be entitled to object to any change in the Sub-Processor and at its discretion (not to be unreasonably exercised) may elect to terminate the Agreement or that part of the Agreement that involves processing of the Protected Data by the Sub-Processor in the event that the Processing Party fails to take the steps suggested by the other party to address the objection and otherwise not cease to use the relevant Sub-Processor;

2.2.3. prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing obligations which offer materially the same level of protection for the Protected Data as those set out in this Addendum, including an obligation on the Sub-Processor to provide sufficient guarantees to implement equivalent technical and organisational measures in accordance with paragraph 3 of this Part 4 and to delete or return the Protected Data in accordance with paragraph 7 of this Part 4. The contract with the Sub-Processor shall state that compliance with the obligations may be enforced by the Processing Party, i including if the other party ceases to exist or becomes insolvent. On request by a party, the Processing Party shall provide a copy of the contract with the Sub-Processor. The Processing Party may redact the text of the contract to the extent necessary to protect confidential information, including any personal data; and

2.2.4. notify the other party of any failure by a Sub-Processor to fulfil its contractual obligations referred to in paragraph 2.2.3 of this Part 4.

2.3. The Processing Party will ensure that all persons authorised by us (or by any Sub-Processor) to process Protected Data are subject to an obligation to keep the Protected Data confidential. The Processing Party shall grant access to the Protected Data to members of the personnel on an "as needed basis" for the Permitted Purposes only.

2.4. The Processing Party will remain fully liable to the other party for any and all acts and omissions of any Sub-Processor, and any persons authorised by us (or by any Sub-Processor) to process Protected Data as if they were their own.

3. Technical and Organisational Measures

3.1. The Processing Party will implement and maintain appropriate technical and organisational measures in accordance with paragraph 2 of Part 1 above, to:

3.1.1. ensure that the processing of Protected Data will meet the minimum requirements of the Data Protection Laws (including as set out in Article 32 GDPR) and ensure the protection of the rights of data subjects; and

3.1.2. provide reasonable assistance to the other party in responding to Data Subject Requests relating to Protected Data.

4. Information and Audit

4.1. Subject to paragraph 4.2 of this Part 4, the Processing Party will, in accordance with Data Protection Laws, as is reasonably necessary to demonstrate our compliance with our obligations under Part 1 – General Terms, this Part 4 – Processor Terms and the Data Protection Laws (unless providing this information would be in breach of Applicable Laws, in which case the Processing Party will inform the other party to the extent it is permitted by Applicable Laws to do so):

4.1.1. as soon as reasonably practicable, make available to the other party the Records, unless providing such information infringes the Data Protection Laws or any Applicable Law (in which case, it will inform the other party to the extent it is permitted by law to do so); and

4.1.2. allow for and contribute to audits, including inspections, by the other party (or an auditor mandated by the other party and agreed by the Processing Party in writing).

4.2. The auditing party will:

4.2.1. provide to the Processing Party reasonable prior written notice (not less than 10 business days) of any information request, audit and/or inspection that a party requires;

4.2.2. ensure that the Records and all information obtained or generated by it or its auditor in connection with such information requests, inspections and audits are kept strictly confidential and it will not disclose the same to a third party unless required to do so by a relevant regulator, in which case, it will (to the extent legally permissible) not less than fourteen (14) days before such disclosure give prior written notice of such requirement to the Processing Party;

4.2.3. ensure that such audit or inspection is undertaken during our normal business hours, with minimal disruption to our business and the business of our other customers;

4.2.4. pay reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits; and

4.2.5. comply with any additional obligations with regard to access by it or an auditor as set out in the Agreement.

4.3. Both parties shall be entitled to share any information referred to in paragraph 4 of this Part 4, including the results of any audit, with a competent Supervisory Authority as may be necessary from time to time.

4.4. Nothing in paragraph 4 of this Part 4 gives the auditing party the right to access any data of any other customer of the Processing Party or any information that could cause the Processing Party to breach its obligations under Applicable Law (including the Data Protection Laws) and/or our confidentiality obligations owed to a third party.

5. Assistance and Data Subject Rights

5.1. The Processing Party is responsible for maintaining a record of Data Subject Requests. Upon receipt of any Data Subject Request, the Processing Party shall immediately (and no later than within 48 (forty-eight) hours of receipt) refer such Data Subject Request to the other party and shall, at its own expense, promptly assist the other party with such Data Subject Request to ensure that the other party meets the response times under the Data Protection Laws. The Processing Party will not respond to a Data Subject Request without providing prior written notice to the other party or as required by Applicable Laws, in which case the Processing Party shall, to the extent permitted by Applicable Laws, inform the other party of that legal requirement prior to it responding to such Data Subject Request.

5.2. The Processing Party will provide such assistance as reasonably required by the other party to ensure compliance with its obligations under the Data Protection Laws with respect to:

5.2.1. security of processing;

5.2.2. data protection impact assessments (as such term is defined in the Data Protection Laws);

5.2.3. prior consultation with a Supervisory Authority regarding high-risk processing;

5.2.4. notifications to the Supervisory Authority and/or communications to data subjects by the Processing Party in response to any Personal Data Breach; and

5.2.5. any remedial action to be taken in response to a Personal Data Breach and/or a Data Complaint or request relating to its obligations under the Data Protection Laws relevant to the Agreement.

Breach Notification

5.3. In respect of any Personal Data Breach, the Processing Party will, without undue delay but in no event later than 48 (forty-eight) hours (or earlier where possible) after becoming aware, notify the other party of the Personal Data Breach and provide the other party with details of the Personal Data Breach including the nature of the Personal Data Breach, the categories and approximate volume of data subjects, the Protected Data records concerned, the likely consequences of the Personal Data Breach and any measures taken or to be taken by it to mitigate the effects of the Personal Data Breach. Where, and insofar as, it is not possible for the Processing Party to provide all of this information at the same time, the initial notification will provide such information as available to it, and it will provide the further information as soon as it becomes available without undue delay (but in no event later than 24 (twenty-four) hours after it becomes available).

5.4. The Processing Party will immediately, at its own expense, investigate the Personal Data Breach and take steps to identify, prevent, mitigate the effects of and remedy any Personal Data Breach. The Processing Party will not release or publish any filing, communication, notice, press release or report concerning any Personal Data Breach without the

other party's prior written approval.

5.5. The Processing Party will promptly (but in no event later than 48 (forty-eight) hours after becoming aware) inform the other if it receives or becomes aware of a Data Complaint and shall not respond to the Data Complaint without the other party's prior written approval.

6. Deletion or Return of Protected Data and Copies

6.1. The Processing Party will process the Protected Data only for the duration of the Data Processing Term, unless a longer period is required under Applicable Laws.

6.2. On termination of the Agreement and, at the other party's written request, the Processing Party will ensure that any Protected Data (and all copies) are securely returned to the other party or destroyed (at its discretion and direction) to the extent reasonably practicable (unless storage is required by Applicable Laws and, if so, the Processing Party will inform the other party of any such requirement) in the following circumstances:

6.2.1. on termination of the Agreement;

6.2.2. on expiry of the Data Processing Term;

6.2.3. once processing of the Protected Data is no longer necessary for the Permitted Purposes.

Schedule 1 - Data Processing Details (Services)

DETAILS OF PROCESSING	DESCRIPTION
SCOPE	The processing of personal data as required for the Permitted Purpose.
NATURE AND PURPOSE	The processing of personal data as required for the Permitted Purpose.
DURATION	For the duration of the Agreement and for such time as required by Applicable Laws (the "**Data Processing Term**").
TYPES OF PERSONAL DATA	Parties will process such categories of personal data as necessary to provide the Services, including the following categories of data: **GENERAL PERSONAL DATA** ● Name ● Age ● Nationality ● Passport number ● Driver's license details ● National identity card details ● Bank account details ● Home address ● Phone number ● Date of birth ● IP address ● Email address ● Personal finances ● Transaction data ● Tax-related matters ● Work-related circumstances ● Qualifications Only where we process Protected Data pursuant to the Services Agreement, we will also process the following categories of personal data: ● Cryptocurrency wallet ID ● Cryptocurrency transaction ID

CATEGORIES OF DATA SUBJECTS	Data subjects include the following individuals associated with you: ● Employees ● Directors ● Shareholders ● Beneficial owners ● Authorised Users ● Partners ● Trustees ● Suppliers ● Customers and End Users ● Job applicants ● Consultants ● Contractors
LOCATIONS OF PROCESSING	● UK ● EU ● US ● Switzerland

Data Processing Details (You, in respect of the Technology and Other Services)

DETAILS OF PROCESSING	**DESCRIPTION**
SCOPE	The processing of personal data as required for the Permitted Purpose.
NATURE AND PURPOSE	The processing of personal data as required for the Permitted Purpose. The data will be processed to provide and improve the Technology and Other Services and in order for you to support Parties otherwise exercise and perform your rights and obligations set out in the Embedded Services Schedule in Section D of the Agreement, including amongst others to support customer verification, fraud, anti-money laundering and crime prevention to facilitate onboarding to the Services and to enable compliance with AML/CFT obligations and to support the other services including engineering and product support and maintenance, customer relationship management, marketing management and data managing and warehousing.
DURATION	For the duration of the Agreement and for such time as required by Applicable Laws (the "**Data Processing Term**").

TYPES OF PERSONAL DATA	Parties will process such categories of personal data as necessary to provide the Services, including the following categories of data: **GENERAL PERSONAL DATA** ● Name ● Home address ● Phone number ● Date of birth ● Signature ● Unique identifiers/personal descriptors ● IP address, cookies/online tracking technologies/Geo location ● Email address ● Tax-related matters ● Communications ● Professional or employment-related information ● Internet or other technical information **SENSITIVE PERSONAL DATA** ● Government-issued identification numbers ● Online account access information, including usernames, passwords, and password recovery information ● Cardholder Data, PANs or other financial account numbers ● Data related to criminal convictions or offences or allegations of crime ● Consumer reporting data, including employment background screening reports ● Details of racial or ethnic origin ● Trade union affiliation ● Genetic data and/or biometric data for the purpose of uniquely identifying a natural person ● Health details ● Information about a person's sex life or sexual orientation
CATEGORIES OF DATA SUBJECTS	Data subjects include the following individuals: ● Customers and end-users
LOCATIONS OF PROCESSING	● UK ● EU ● Switzerland ● US ● Singapore
NAMES OF SUB-PROCESSORS - Embedded Partner (if applicable)	See details in the Commercial Terms annexed to the Agreement.

LOCATIONS OF PROCESSING BY YOUR SUB-PROCESSORS **- Embedded Partner (if applicable)**	See details in the Commercial Terms annexed to the Agreement.

Schedule 2 - Security Measures

1. The security measures include:

1.1 ensuring access to the Protected Data by all persons authorised to process the Protected Data is on an "as needed" basis, using user and logical-based segmentation and controls (including conditional access, two-factor authentication, just in time for privileged access);

1.2 pseudonymising and/or encrypting the Protected Data stored by a party or transmitted by a party over public or wireless networks; and

1.3 implementing and maintaining business continuity, disaster recovery and other relevant policies and procedures to ensure the confidentiality, integrity, availability and resilience of processing systems and services and the availability and access of Protected Data in a timely manner in the event of a physical or technical incident.

Schedule 3 - Cross-Border Data Transfer Mechanisms

1. Definitions

1.1. Terms used in this Schedule 3 shall have the meanings set out below, in the Addendum or as otherwise defined in the UK International Data Transfer Addendum or EU Standard Contractual Clauses. Where a term is defined in both this Schedule 3 and the UK International Data Transfer Agreement or the EU Standard Contractual Clauses, the meaning of the term in the UK International Data Transfer Agreement or the EU Standard Contractual Clauses (as applicable) shall have precedence in relation to the UK International Data Transfer Agreement or the EU Standard Contractual Clauses (as applicable).

"**EU Standard Contractual Clauses"**	means the Standard Contractual Clauses approved by the European Commission in decision 2021/914; and
"**UK International Data Transfer Agreement**"	means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross-Border Data Transfer Mechanisms

2.1. **Order of Precedence.** In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses as set forth in paragraph 2.2 (EU Standard Contractual Clauses) of this Schedule 3; (b) the UK International Data Transfer Agreement as set forth in paragraph 2.3 (UK International Data Transfer Agreement) of this Schedule 3; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Data Protection Laws.

2.2. **EU Standard Contractual Clauses**. The EU Standard Contractual Clauses will apply to personal data that is transferred via the Services from the EEA, Switzerland, Guernsey, or Jersey, either directly or via onward transfer, to any country or recipient outside the EEA, Switzerland, Guernsey, or Jersey that is not recognised by the relevant competent authority as providing an adequate level of protection for personal data. For data transfers that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into, and incorporated into this Addendum by this reference, and the following modules may apply depending on whether a party acts as a controller, joint controller or processor of personal data:

2.2.1. module One (Controller to Controller) of the EU Standard Contractual Clauses;
2.2.2. module Two (Controller to Processor) of the EU Standard Contractual Clauses;
2.2.3. module Three (Processor to Processor) of the EU Standard Contractual Clauses;
2.2.4. module Four (Processor to Controller) of the EU Standard Contractual Clauses; and
2.2.5. for each module, where applicable, the modules will be completed as follows:

2.2.5.1. in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;
2.2.5.2. in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply, and the time period for prior written notice of sub-processor changes will be as outlined in paragraph 2.2.2 in Part 4 - Processor Terms of this Addendum;
2.2.5.3. in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

2.2.5.4. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

2.2.5.5. in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

2.2.5.6. in Annex I, Part A of the EU Standard Contractual Clauses:

Data Exporter:	
Us	
Contact details:	Our data protection team: dpo@bvnk.com
Data Exporter Role:	The Data Exporter's role is set forth in the table on page 1 of this Data Processing Addendum to the Agreement.
Signature and Date:	By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
You	
Contact details:	As set out in the Agreement.
Data Exporter Role:	The Data Exporter's role is set forth in the table on page 1 of this Data Processing Addendum to the Agreement.
Signature and Date:	By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
Data Importer:	
Us	
Contact details:	Our data protection team: dpo@bvnk.com
Data Importer Role:	The Data Importer's role is set forth in the table on page 1 of this Data Processing Addendum to the Agreement.
Signature and Date:	By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
You	
Contact details:	As set out in the Agreement.
Data Importer Role:	The Data Importer's role is set forth in the table on page 1 of this Data Processing Addendum to the Agreement.
Signature and Date:	By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

2.2.5.7. in Annex I, Part B of the EU Standard Contractual Clauses:

2.2.5.7.1. the categories of data subjects are set forth in Schedule 1 (Data Processing Details) of this Addendum;

2.2.5.7.2. the frequency of the transfer is on a continuous basis for the duration of the Agreement;

2.2.5.7.3. the nature of the processing is set forth in the table in Schedule 1 (Data Processing Details) of this Addendum;

2.2.5.7.4. the purpose of the processing is set forth in the table in Schedule 1 (Data Processing Details) of this Addendum;

2.2.5.7.5. the period for which the personal data will be retained is set forth in the table in Schedule 1 (Data Processing Details) of this Addendum;

2.2.5.7.6. for transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth at our Help Centre;

2.2.5.8. in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority; and

2.2.5.9. Schedule 2 (Security Measures) of this Addendum serves as Annex II of the EU Standard Contractual Clauses.

2.3. **UK International Data Transfer Agreement**. The parties agree that the UK International Data Transfer Agreement will apply to personal data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into, and incorporated into this Addendum by this reference, and completed as follows:

2.3.1. In Table 1 of the UK International Data Transfer Agreement, the Customer's and our details and key contact information are set forth in paragraph 2.2.5.6 of this Schedule 3;

2.3.2. In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules, and selected clauses, which the UK International Data Transfer Agreement is appended to, are set forth in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 3;

2.3.3. In Table 3 of the UK International Data Transfer Agreement:

2.3.3.1. the list of Parties is set forth in paragraph 2.2.5.6 of this Schedule 3;

2.3.3.2. the description of the transfer is set forth in the table in Schedule 1 (Data Processing Details);

2.3.3.3. annex II is located in Schedule 2 (Security Measures) of this Addendum;

2.3.3.4. the list of sub-processors is available at our Help Centre or as otherwise provided by you to us; and

2.3.3.5. in Table 4 of the UK International Data Transfer Agreement, both the importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.4. **Conflict**. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, the Agreement, or the Privacy Policy, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.