Data Protection Clauses (Addendum)

This Addendum is incorporated into and forms part of the agreement between ClearBank Limited (**ClearBank, we, us** and **our**) and you (each a **party** and together the **parties**). In the event of any conflict between this Addendum and the other provisions of the Agreement, or the ClearBank Privacy Notice, this Addendum will prevail.

1 DEFINITIONS AND INTERPRETATION

1.1 The following definitions and rules of interpretation apply in this Addendum (unless the context otherwise requires):

Agreement	means the agreement between us and you which incorporates this Addendum by reference;
Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of personal data as may be permitted under the Data Protection Legislation from time to time, including those set out in Article 46 GDPR and the implementation of binding corporate rules pursuant to Article 47 GDPR;
Business Day	means a day, other than Saturday, Sunday, or public holiday in England (or, if applicable, in Jersey) when banks in London (or, if applicable, in Jersey) are open for business;
Client	means your client or the end user who will use or benefit from the Services;
Commencement Date	means the effective date of the Agreement;
Controller Data	has the meaning given to that term in Part 3 - Controller Terms of this Addendum;
Data Complaint	means a complaint or request relating to either party's obligations under the Data Protection Legislation relevant to the Agreement, including any complaint by a data subject or any notice, investigation, or other action by a Supervisory Authority;
Data Protection Legislation	means (i) any legislation in force from time to time relating to privacy and/or the processing of personal data including the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 (GDPR), the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and any laws or regulations implementing the Privacy and Electronic Communications Directive 2002/58/EC; (ii) any laws which replace, extend, re-enact, consolidate or amend any of the foregoing whether or not before or after the date of the Agreement from the date they come into force (except, where permissible under applicable domestic law, to the extent that the GDPR is modified by applicable domestic law from time to time but where the modification has the effect of depriving data subjects of rights to which they would otherwise be entitled were any relevant processing be carried out in the EEA; such modification will have no effect on this Agreement); and (iii) the guidance and codes of practice issued by any relevant EEA Supervisory Authority and applicable to a party;

Data Subject Request	means a request made by a data subject to exercise any rights of data subjects under the Data Protection Legislation;
Direct Third-Party Service	means any service (or elements of such service) that is not provided by us under the Agreement and is instead provided wholly by a third party provider and in respect of which you have entered or will enter into a direct agreement with the relevant third party provider in respect of that service;
Direct Third-Party Service Provider	means a third party, including a TPP, that provides Direct Third-Party Services and with whom you have entered or will enter into a direct agreement in respect of those Direct Third-Party Services;
EEA	means the member states of the European Union together with Iceland, Liechtenstein and Norway;
GDPR	means Regulation (EU) 2016/679 of the European 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;
Group	means, in relation to a company, that company, any subsidiary or holding company from time to time of that company and any subsidiary from time to time of a holding company of that company where the terms *subsidiary* and *holding company* are as defined in section 1159 of the Companies Act 2006*;*
Joint Data	has the meaning given to that term in Part 2 - Joint Controller Terms of this Addendum;
Permitted Purpose	has the meaning given to that term in Part 1 – General Terms;
Personal Data	means any and all personal data that is processed by us pursuant to or in connection with the Agreement irrespective of our role, including Joint Data, Controller Data and Processor Data;
Personnel	means, in respect of a party or a member of its Group, their directors, officers, employees, consultants, agents, servants and contractors and such persons of their sub-contractors (as applicable to each party);
Portal	means the ClearBank online service management portal made available to you by us from time to time;
Privacy Notice	means ClearBank's privacy notice which is available on the Portal and the Website and which may be updated from time to time by ClearBank;
Processing Instructions	has the meaning given to that term in paragraph 1 of Part 4 – Processor Terms of this Addendum;
Processor Data	has the meaning given to that term in Part 4 - Processor Terms of this Addendum;

Relevant Laws	means any laws, regulations, regulatory constraints, obligations or rules in the United Kingdom, or any other relevant jurisdiction, which are applicable to this Agreement (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 any Relevant Regulatory Authority;
Relevant Payment System Operator	means, as provided in Section 42(3) of the Financial Services Banking Reform Act 2013, a person with responsibility under a payment system for managing or operating it, including its management;
Relevant Regulatory Authority	means a regulatory authority with jurisdiction over one or both of the parties in relation to the provision or receipt of the Services or performance of the parties' obligations under the Agreement, including the UK Financial Conduct Authority, the UK Prudential Regulatory Authority, the Bank of England, the European Commission, HM Treasury, the UK Competition and Markets Authority, any tax authority, a payment systems regulator and any Supervisory Authority;
Services	means any services provided by us to you under the Agreement from time to time;
Sub-Processor	means another processor engaged by us for carrying out processing activities in respect of the Processor 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 Legislation including the Information Commissioner's Office;
TPP	means a third party provider under the Payment Services Regulations 2017 (SI 2017/752) (PSR) which may be any of an AISP, a PISP and/or a CBPII (all as defined in the PSR); and
Website	means www.clear.bank.

1.2 Lowercase terms used but not defined in this Addendum such as "*personal data*", "*personal data breach*", "*processing*", "*processor*", "*controller*", "*joint controller*" and "*data subject*" have the meanings set out in the Data Protection Legislation.

1.3 Unless the context otherwise requires, and subject to the definition of Data Protection Legislation in clause 1.1 above, any reference to European Union law that is directly applicable or directly effective in the United Kingdom at any time is a reference to it as it applies in the EEA from time to time, including as retained, amended, extended or re-enacted or otherwise given effect on or after 31 January 2020.

1.4 Where we refer to "*you*" or "*your*", we mean your business or organisation. If two or more persons are comprised in the expression "*you*" or "*your*", we mean each person separately and all of them jointly.

1.5 References in this Addendum to paragraphs are to paragraphs of this Addendum and references to Parts are to the Parts of this Addendum.

1.6 Any phrase introduced by the terms "*including*", "*include*", "*in particular*" or any similar expression will be construed as illustrative and will not limit the sense of the words preceding those terms.

1.7 We reserve the right to update this Addendum from time to time including in order to comply with our obligations under the Data Protection Legislation, to address any changes to the Services including any new functionality or features and/or to cover any additional services that we may provide to you from time to time. The prevailing terms will be the terms of the most recent version of this Addendum made available on the Portal and the Website and notice will be deemed to be given on the date of publication on the Portal and the Website.

2 ClearBank's Role

2.1 In providing the Services and otherwise complying with its obligations under the Agreement, we may act as a joint controller, a controller, or a processor of personal data.

2.2 This Addendum is divided into the following parts:

2.2.1 **Part 1 General Terms** – these terms apply irrespective of our role;

2.2.2 **Part 2 Joint Controller Terms** – these terms apply only where we act as a joint controller;

2.2.3 **Part 3 Controller Terms** – these terms apply only where we act as an independent controller;

2.2.4 **Part 4 Processor Terms** – these terms apply only where we act as a processor.

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, 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.

Part 1 - General Terms

1 Data Processing

1.1 We will process personal data as required in the provision or receipt of the Services, or in contemplation of the provision of any services by us, for the performance and exercise of our rights and obligations under the Agreement, for our legitimate business purposes (including compliance with our legal and regulatory obligations, IT security and administration purposes) and as further detailed in the Privacy Notice (**Permitted Purpose**).

1.2 We will maintain any valid registrations and pay any fees as required by our national Supervisory Authority to cover the processing activities contemplated for the Permitted Purpose.

1.3 We have a Data Protection Officer and any queries relating to this Addendum and/or the processing of personal data by us should be sent to our Data Protection Officer at DataProtectionOfficer@Clear.Bank.

2 Data Security

2.1 We have developed the Services with IT security and the Data Protection Legislation in mind.

2.2 We have, and will maintain, appropriate technical and organisational measures to ensure the security, integrity, availability and confidentiality of the Personal Data and protect against unauthorised or unlawful processing of the Personal Data and the accidental loss or destruction of, or damage to, the Personal Data, such measures to be appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction of, or damage to, the Personal Data and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures.

2.3 We have the following measures in place:

2.3.1 **Access Controls** – access to the Personal Data by our Personnel is on an "as needed" basis using user and logical based segmentation and controls (including conditional access, multi factor authentication, and just in time for privileged access). Access is granted on a 'role/activity based' approach and implements least privilege access mechanisms and segregation of duties;

2.3.2 **Encryption** – encryption of Personal Data at rest and in transit;

2.3.3 **Monitoring and Testing** – Real time SIEM monitoring, daily external scanning of the ClearBank environment, internal vulnerability scanning and extensive penetration testing and we act to reasonably remediate any vulnerabilities identified because of such monitoring and testing;

2.3.4 **Data Leakage Prevention Measures** – systems are in place to block and prevent any transfer of data that might result in a personal data breach; and

2.3.5 **Data Backup** – Data is backed up according to an agreed backup schedule.

2.4 Where we engage an external party to review or audit any of our information security measures, or perform such review or audit ourselves, we will, or we shall ensure that the external party will, provide you with a summary of any conclusions drawn or recommendations made. Additionally, you will be able to review, on request, complete copies of recommendations or conclusions online, using Webex or a similar system.

2.5 Where we become aware of any vulnerability in relation to the technical and organisational measures referred to in paragraph 2.2 above, we will promptly advise you about such vulnerability and take all reasonable steps necessary, in our opinion, to mitigate or remove any such vulnerability and keep you informed of all such progress.

2.6 Where you become aware of any potential vulnerability in relation to the technical and organisational measures referred to in paragraph 2.2 above, you will promptly advise us about such potential vulnerability and we will take all reasonable steps necessary, in our opinion, to mitigate or remove any such vulnerability and keep you informed of all such progress.

2.7 We are ISO 27001 certified and have implemented a risk assessment framework that is based on the principle of ISO31000 and the NIST Framework.

2.8 We have and will maintain adequate data processing, privacy and IT security policies in relation to the processing of personal data and any cyber security incident that meets the requirements of the Data Protection Legislation and we will procure that our Personnel comply, at all times, with such policies.

2.9 Our Personnel are subject to written confidentiality obligations which cover their processing of any Personal Data.

3 Training

3.1 We will ensure that our Personnel are appropriately trained to process the Personal Data in accordance with the Data Protection Legislation. The level, content and regularity of such training will be proportionate to the Personnel's role, responsibility, and frequency with respect to their processing of Personal Data. We will maintain, and regularly review, records of training undertaken by our Personnel. At a minimum, all staff receive annual training in relation to Data Protection Legislation and the processing of Personal Data.

4 Using Staff and other Processors

4.1 We will not engage a Processor or Sub-Processor to carry out any processing activities in respect of Personal Data without your prior specific or general consent and subject to our compliance with paragraphs 4.2 and 4.3 of this Part 1 – General Terms.

4.2 We will:

4.2.1 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 Personal Data as those set out in this Part 1 – General Terms.

4.2.2 notify you fourteen (14) days in advance before engaging any Processor or Sub-Processor that we have not previously communicated to you (via our relevant policies or otherwise) by directing you to an updated list of Processors or Sub-Processors (or otherwise). If you wish to object to the engagement of such new Processor or Sub-Processor you must provide us with written notice of such objection including reasonable details of the grounds for your objection (**Objection Notice**) as soon as possible. Following receipt of an Objection Notice, we will endeavour to discuss any reasonable objections with you in good faith. If, after 61 days from the date on which we received the Objection Notice, you can demonstrate that we have failed to comply with paragraph 4.2.1 of this Part 1 – General Terms , then you may terminate the Agreement by giving us notice in writing addressed to legalnotices@clear.bank and in accordance with the terms of the Agreement,

and we will 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.

4.3 We will ensure that all persons authorised by us (or by any Processor or Sub-Processor) to process Personal Data are subject to an obligation to keep the Personal Data confidential (except where disclosure is required in accordance with Relevant Laws, in which case we will, where practicable and not prohibited by Relevant Laws, notify you of any such requirement before such disclosure).

4.4 You consent to our use of the Processors or Sub-Processors set out in Schedule 1 of this Addendum, subject to our compliance with paragraph 4.2.1 of this Part 1 – General Terms.

5 Records and Audits

5.1 We will document and maintain accurate, complete, and up to date records of our processing activities in accordance with the requirements of the Data Protection Legislation (**Records**).

5.2 Subject to paragraph 5.3 of this Part 1 – General Terms, we will, in accordance with the Data Protection Legislation and as is reasonably necessary to demonstrate our compliance with our obligations under this Addendum and the Data Protection Legislation:

5.2.1 make available to you the Records (unless providing this information would be in breach of Relevant Laws, in which case, we will inform you to the extent we are permitted by Relevant Laws to do so); and

5.2.2 allow for and contribute to audits, including inspections, by you (or an auditor mandated by you and agreed by us in writing).

5.3 You will:

5.3.1 provide to us reasonable prior written notice (not less than 10 Business Days) of any information request, audit and/or inspection that you require;

5.3.2 ensure that the Records and all information obtained or generated by you or your auditor in connection with such information requests, inspections and audits are kept strictly confidential and you will not disclose the same to a third party unless required to do so by a Relevant Regulatory Authority, in which case, you will (to the extent legally permissible) not less than fourteen (14) days before such disclosure give prior written notice of such requirement to us;

5.3.3 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;

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

5.3.5 comply with any additional obligations with regards to access by you or an auditor as set out in the Agreement.

5.4 Nothing in paragraph 5 of this Part 1 – General Terms, gives you the right to access any data of any other customer of ours or any information that could cause us to breach our obligations under Relevant Laws (including the Data Protection Legislation) and/or our confidentiality obligations owed to a third party.

6 Data Transfers

6.1 We will not transfer the Personal Data to a country or territory outside of the European Economic Area (and the United Kingdom when the United Kingdom ceases to be part of the European Economic Area) including to a Sub-Processor located in such a country or territory unless:

6.1.1 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 Legislation;

6.1.2 we have ensured that any such transfer complies with the Data Protection Legislation by having in place Appropriate Safeguards and we have taken steps to satisfy ourselves that:

6.1.2.1 the level of protection afforded to the Personal Data in the destination country or territory is equivalent to the level of protection that would be afforded to Personal Data in the EEA;

6.1.2.2 any data importer shall provide us 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 6.1.2.1; and

6.1.2.3 any data importer is contractually obliged to keep us informed of any development affecting or likely to affect the level of protection your transferred Personal Data receives in the importer's country; or

6.1.3 we are otherwise permitted to do so by virtue of a derogation in Article 49 of the GDPR or as otherwise provided under the Data Protection Legislation.

6.2 If, for whatever reason, the transfer of Personal Data pursuant to paragraphs 6.1.1, 6.1.2 or 6.1.3 of this Part 1 – General Terms ceases to be lawful, we will immediately implement other Appropriate Safeguards and ensure that the level of protection afforded to the Personal Data in the destination country or territory is equivalent to the level of protection that would be afforded to Personal Data in the EEA. Where we cannot do that, we will cease any such transfer of Personal Data unless you expressly authorise the transfer to continue.

7 Data Retention

7.1 We will not retain Personal Data for longer than is necessary to carry out any Permitted Purpose.

7.2 We will maintain and comply with our data retention policy, details of which we will provide to you on written request.

8 Reporting

8.1 We will comply with our obligations under the Data Protection Legislation to report a personal data breach to the appropriate Supervisory Authority and (where applicable) to data subjects.

8.2 We will notify you promptly (and in any event within 48 (forty eight) hours) if we become aware of a personal data breach by us or otherwise in connection with the Services and provide you with full details of the personal data breach. We will provide reasonable co-operation and

assistance to you as is necessary to facilitate the handling of a personal data breach in an expeditious and compliant manner and to enable us to comply with our obligations under the Data Protection Legislation. We will not release or publish any filing, communication, notice, press release or report concerning any personal data breach by us or otherwise in connection with the Services unless required to do so under the Data Protection Legislation and/or by a Supervisory Authority, in which case, we will notify you in advance of such requirement;

8.3 We will take prompt action to investigate any personal data breach involving Personal Data and to identify, prevent and mitigate the effects of and to remedy any such personal data breach.

8.4 We will act reasonably to keep you informed of ongoing developments in relation to any personal data breach.

9 Your Obligations

9.1 Irrespective of whether we act as a joint controller, controller, or processor:

9.1.1 you are solely responsible for making an independent determination as to whether the technical and organisational measures implemented by us are adequate and meet the requirements of the Data Protection Legislation and any other obligations you have under Relevant Laws;

9.1.2 you will comply, at all times, with your obligations as a controller or joint controller (as applicable) and will provide your services to Clients in compliance with the Data Protection Legislation;

9.1.3 you will maintain any valid registrations and pay any fees as required by your Supervisory Authority to cover your processing activities including those contemplated under the Agreement;

9.1.4 you will maintain adequate data processing, privacy and IT security policies in relation to your processing of personal data and any cyber security incident, that meet the requirements of the Data Protection Legislation and you will comply with and procure that your Personnel comply at all times with, such policies;

9.1.5 you will ensure that your Personnel are subject to written confidentiality obligations which cover their processing of Personal Data;

9.1.6 you will provide all necessary, fair and transparent information and notices to, and obtain all necessary consents from, any data subjects whose personal data you provide to us (including Personnel, Direct Third Party Service Providers and Clients), so that we are lawfully able to use or otherwise process this personal data for the Permitted Purpose without needing any further consent, approval or authorisation, and upon our request from time to time, you will consult with us, and comply with our reasonable requests in relation to the same. You will ensure that such information and notices detail the purposes of processing of personal data as required for the Permitted Purpose, the legal basis for such processing, the recipients of the personal data (including us, Relevant Payment System Operators and Relevant Regulatory Authorities and such other third parties as identified in the Privacy Notice) and such other information as required to be given by a controller to data subjects under the Data Protection Legislation;

9.1.7 if requested by us, you will promptly provide reasonable evidence to us that you have provided all necessary information and notices to and obtained all necessary consents from data subjects and otherwise complied with your obligations under the Data Protection Legislation;

9.1.8 we will be entitled to assume that any disclosure or transfer of personal data to us by you (directly or indirectly) is done so in a manner which is compliant with the Data Protection Legislation;

9.1.9 you will ensure that any personal data you disclose or otherwise transfer to us is accurate;

9.1.10 you will not disclose or transfer to us, any excessive or irrelevant personal data that is not required by us in connection with the performance of the Services or otherwise for the Permitted Purpose and you will ensure that you delete from any documents that you disclose or transfer to us any such excessive or irrelevant personal data;

9.1.11 you will notify us promptly (and in any event within 48 (forty eight) hours) if you become aware of a personal data breach by us or otherwise in connection with the Services and provide us with full details of the personal data breach. You will provide reasonable co-operation and assistance to us as is necessary to facilitate the handling of a personal data breach in an expeditious and compliant manner and to enable us to comply with our obligations under the Data Protection Legislation. You will not release or publish any filing, communication, notice, press release or report concerning any personal data breach by us or otherwise in connection with the Services unless required to do so under the Data Protection Legislation and/or by a Supervisory Authority, in which case, you will notify us in advance of such requirement;

9.1.12 you will notify us promptly (where legally permissible and within no more than 2 (two) Business Days) if you receive or become aware of a Data Complaint and you will provide reasonable co-operation and assistance to us as is necessary to deal with such Data Complaint;

9.1.13 you will provide us with reasonable co-operation and assistance as may be required from time to time to enable us to comply with our obligations under the Data Protection Legislation including those obligations relating to security, Data Subject Requests, data protection impact assessments and consultations with a Supervisory Authority; and

9.1.14 you will comply with any additional obligations imposed on you in the other Parts of this Addendum.

Part 2 - Joint Controller Terms

Where the parties process personal 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, 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 Legislation 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 Legislation 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, Relevant Payment System Operators and Relevant Regulatory Authorities) and such other information as required to be given by a controller to data subjects under the Data Protection Legislation. Such information and notices will be transparent as to the arrangement between the parties in compliance with the Data Protection Legislation;

1.2.5 it will co-operate 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 Legislation with respect to security, personal data breach notifications, data protection impact assessments and consultations with Supervisory Authorities, in so far 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 2 (two) Business Days 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 Legislation (including with respect to any timescales).

2.5 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 Legislation 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 co-operate 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, we 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 you become aware of a personal data breach in relation to the Joint Data, you will notify us by email at DataProtectionOfficer@Clear.Bank.

Part 3 - Controller Terms

Where ClearBank processes personal 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, in addition to Part 1 – General Terms.

1 Processing Controller Data

1.1 We will comply with our controller obligations under the Data Protection Legislation in connection with our processing of Controller Data.

1.2 We 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 details the processing of personal data as required for the Permitted Purpose, the legal basis for such processing, the recipients of the personal data (including Relevant Payment System Operators and Relevant Regulatory Authorities) and such other information as required to be given by a controller to data subjects under the Data Protection Legislation; 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 you receive a Data Subject Request and/or a Data Complaint relating to the processing of Controller Data, to the extent legally permissible, you will promptly notify us (and in any event within 2 (two) Business Days of receipt of the Data Subject Request and/or Data Complaint) by email at DataProtectionOfficer@Clear.Bank and, unless otherwise required under Relevant Laws or by a Supervisory Authority, we, as controller, will be responsible for and will handle such Data Subject Request and/or Data Complaint in compliance with the Data Protection Legislation.

Part 4 - Processor Terms

Where ClearBank processes personal data as a processor for you under or otherwise in connection with the Agreement (**Processor Data**), the provisions set out in this Part 4 Processor Terms will apply to the processing of Processor Data, in addition to Part 1 – General Terms.

1 Instructions and Details of Processing

1.1 In performing our obligations as a processor, we will, unless required to do otherwise by Relevant Laws, process the Processor Data only on and in accordance with the Agreement, Schedule 1 and any other documented instructions from you, all as updated from time to time (**Processing Instructions**).

1.2 If Relevant Laws require us to process Processor Data other than in accordance with the Processing Instructions, we will notify you of any such requirement before processing the Processor Data (unless Relevant Laws prohibits such information on important grounds of public interest).

2 Technical and Organisational Measures

2.1 We will implement and maintain appropriate technical and organisational measures to:

2.1.1 ensure that the processing will meet the requirements of the Data Protection Legislation (including as set out in Article 32 GDPR) and ensure the protection of the rights of data subjects; and

2.1.2 provide reasonable assistance to you in responding to Data Subject Requests relating to Processor Data.

3 Assistance and Data Subject Rights

3.1 If we receive a Data Subject Request relating to the processing of Processor Data then, to the extent legally permissible, we will promptly notify you (and in any event within 2 (two) Business Days of receipt of the Data Subject Request) and, unless otherwise required under Relevant Laws or by a Supervisory Authority, you are responsible for and will handle such Data Subject Request in compliance with the Data Protection Legislation. We will reasonably co-operate and assist you in executing your obligations under the Data Protection Legislation in relation to such Data Subject Request.

3.2 We will provide such assistance as you reasonably require (considering the nature of processing and the information available to us) to assist you in executing your obligations under the Data Protection Legislation with respect to:

3.2.1 security of processing;

3.2.2 data protection impact assessments (as such term is defined in Data Protection Legislation);

3.2.3 prior consultation with a Supervisory Authority regarding high risk processing;

3.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by you in response to any personal data breach; and

3.2.5 any remedial action to be taken in response to a personal data breach.

4 Information and Audit

4.1 We will, in accordance with Data Protection Legislation, make available to you such information as is reasonably necessary to demonstrate our compliance with the obligations of processors under this Part 4 – Processor Terms and the Data Protection Legislation (unless providing this information would be in breach of Relevant Laws, in which case we will inform you to the extent we are permitted by Relevant Laws to do so) and will allow for and contribute to audits, including inspections, by you (or an auditor mandated by you and agreed by us in writing) for such purpose (including where required by a Supervisory Authority) subject to you complying with Part 1 – General Terms paragraphs 5.3 and 5.4 above.

5 Deletion or return of Processor Data and copies

5.1 On termination of the Agreement, and at your written request, we will return any Processor Data to you or, at your option, securely destroy it to the extent reasonably practicable (unless storage of any Processor Data is required by Relevant Laws, in which case we will be entitled to retain the same in accordance with Relevant Laws).

SCHEDULE 1
Part 1 - Data Processing Details

Detail	**Description**
Subject matter of the Personal Data Processing	The processing of personal data as required for the Permitted Purpose.
Duration of the Personal Data Processing	For the duration of the Agreement and for such time as required by Relevant Laws.
The nature and purpose of the Personal Data Processing	The processing of personal data as required for the Permitted Purpose.
The type of Personal Data Processing	Personal data relating to individuals that is provided to ClearBank or otherwise obtained by ClearBank for the Permitted Purpose including identity data, contact data, financial data, transaction data, correspondence data, usage data (for the Portal and Website), security data (e.g. passwords, username) technical data, publicly available data (e.g. data in public records) and marketing and communications data (all as further detailed in the Privacy Notice).
The categories of Data Subject	Individuals about whom personal data is provided by or at your direction, any individual associated with you which includes partners, directors, shareholders, beneficial owners, company secretaries, trustees, members and employees and anyone whose personal data ClearBank processes in connection with the Services or in contemplation of the provision of services or otherwise for the Permitted Purpose including Clients, payers, and payees.

Part 2 - Approved Processors or Sub-Processors

Freshworks Inc.

Napier Technologies Limited

LexisNexis Risk Solutions (UK) Ltd

Opsmatix Systems Limited

ThetaRay Ltd

RingCentral UK Limited