

Data Protection Addendum (Addendum)

This Addendum is incorporated into and forms part of the agreement entered into between ClearBank Limited (**ClearBank, we, us and our**) and the customer/client identified in the agreement (**Customer, you, and your**) (each a **party** and together the **parties**). In the event of any conflict between this Addendum and the other provisions of the Agreement relating to data protection, this Addendum will prevail to the extent of such conflict unless expressly agreed otherwise in writing by the parties.

1 DEFINITIONS AND INTERPRETATION

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

Adequacy Decision	means a valid adequacy decision or adequacy regulations pursuant to Article 45 of the EU GDPR or the UK GDPR (as appropriate);
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 a 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;
Commissioner	means the UK's Information Commissioner's Office;
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 and applicable to a party, the Services or the Agreement including the Data Protection Act 2018, the UK GDPR, the Gibraltar GDPR and Data Protection Act 2004, the EU

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 (where applicable); (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 UK GDPR or Gibraltar 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 Supervisory Authority and applicable to a party. In the event of any conflict between the definition of Data Protection Legislation in this Addendum and the definition in the Agreement, the definition in this Addendum shall prevail for the purposes of this Addendum and the Agreement;

Data Subject Request	means a request made by a data subject to exercise any rights of data subjects under the Data Protection Legislation relating to Controller Data, Joint Data, Processor Data or Protected Data (as the context requires);
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;
DTA	means the data transfer appendix defined in Part 1 – General Terms paragraph 6.3 and which sets out the Appropriate Safeguards for a Restricted Transfer;
EEA	means the member states of the European Union together with Iceland, Liechtenstein, and Norway;
EU 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;

Gibraltar GDPR	has the meaning set out in section 2(1) of Gibraltar’s Data Protection Act 2004;
GDPR	means the UK GDPR, Gibraltar GDPR or the EU GDPR (as applicable to the processing of personal data pursuant to the Agreement);
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 <i>subsidiary</i> and <i>holding company</i> 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 Data Purpose(s)	has the meaning given to that term in paragraph 1.1 of Part 1 – General Terms or in paragraph 1.1 of Part 5 – Customer Processor Terms or means such purposes as set out in the Agreement (as applicable);
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, Processor Data and Protected Data (as the context requires);
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 1.1 of Part 4 – Processor Terms or in paragraph 1.1 of Part 5 – Customer Processor Terms of this Addendum (as appropriate);
Processor Data	has the meaning given to that term in Part 4 - Processor Terms of this Addendum;
Protected Data	means any and all personal data processed by you as a processor on behalf of ClearBank (acting as a controller) pursuant to or in connection with the Agreement;
Records	means accurate, complete, and up to date records of our processing activities relating to Personal Data carried out

in connection with, or for the purposes of, the Agreement as required under the Data Protection Legislation;

Relevant Laws	means any laws, regulations, regulatory constraints, obligations or rules in the United Kingdom (or any part of the United Kingdom), or any other relevant jurisdiction (including in the European Union or any member state of the European Union to the extent that the EU GDPR applies to the processing of Personal Data), 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;
Restricted Transfer	means a transfer of personal data which is covered by Chapter V of the GDPR but which is not to a territory covered by an Adequacy Decision and which is made between the parties pursuant to or in connection with the Agreement;
Services	means any services provided by us to you or by you to us (as the context requires) under the Agreement from time to time;
Sub-Processor	means another processor engaged by us or by you when acting as a processor (as the context requires) for carrying out processing activities under or in connection with the Agreement;
Supervisory Authority	means any relevant 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 Commissioner;

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
UK GDPR	has the meaning set out in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018;
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 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.
- 1.4 References in this Addendum to paragraphs are to paragraphs of this Addendum and references to Parts are to the Parts of this Addendum. The Schedule and Appendix form part of this Addendum and references to the Addendum include the Schedule and Appendix and any additional appendices or documents referenced herein.
- 1.5 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.
- 1.6 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 to you on the date of publication on the Portal and the Website.

2 ClearBank's Role

- 2.1 In providing or receiving 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 and you 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;
- 2.2.5 **Part 5 - Customer Processor Terms** – these terms apply only where you act as a processor for ClearBank acting as a controller.

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 or Part 5 – Customer Processor Terms**, the provisions in **Part 2 – Joint Controller Terms, Part 3 – Controller Terms, Part 4 – Processor Terms or Part 5 – Customer Processor Terms** (as applicable) will prevail to the extent of the conflict.

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 verification, fraud and crime prevention, 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, administration, business development and marketing purposes) and as further detailed in the Privacy Notice (**Permitted Data Purposes**).
- 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 Data Purposes.
- 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 we provide 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 security 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** – Annual data recovery 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 **Mutual Authentication** – use of mTLS authentication;
 - 2.3.5 **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
 - 2.3.6 **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 on request, or we shall ensure that the external party will on request, 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 warrant that we have ISO 27001:2013 and ISAE3402 certification, or similar best practice security controls in place and will maintain these security controls during the term of the Agreement.
 - 2.8 We have and will maintain adequate data processing, privacy, and IT security policies in relation to our processing of Personal Data and any cyber security incident that meet the requirements of the Data Protection Legislation and we will procure that our Personnel comply, at all times, with such policies.

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 the GDPR and the processing of personal data.

4 Using Staff and other Processors

- 4.1 We will ensure that all persons authorised by us (or by any processor or Sub-Processor) to process Personal Data (including Personnel) are subject to an obligation to keep the Personal Data confidential.

5 Records and Audits

- 5.1 We will document and maintain 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 independent auditor mandated by you and agreed by us in writing).

- 5.3 You will:

5.3.1 take into account our security certifications (including those set out in paragraph 2 of this **Part 1 – General Terms**) when deciding whether to carry out a review or audit;

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

5.3.3 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;

5.3.4 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;

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

5.3.6 comply with any additional obligations with regards to access by you or an auditor including any security policies notified by us to you or 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 United Kingdom, Gibraltar or the European Economic Area including to a Sub-Processor located in such a country or territory unless:

- 6.1.1 there is an Adequacy Decision in respect of that country or territory; or
- 6.1.2 in the case of a Restricted Transfer, we have ensured that any such transfer complies with the Data Protection Legislation by having in place Appropriate Safeguards; 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 UK (where the UK GDPR applies to the transfer), Gibraltar (where the Gibraltar GDPR applies to the transfer) or the EEA (where the EU GDPR applies to the transfer). Where we cannot do that, we will cease any such transfer of Personal Data.

6.3 If you are located outside the UK, Gibraltar and the EEA and we need to transfer the Personal Data to you pursuant to the Agreement, and such transfer is a Restricted Transfer, either:

- 6.3.1 we will enter into a data transfer appendix (in substantially the form of the data transfer appendix set out in the Appendix) to provide for Appropriate Safeguards as agreed and signed between us and you which shall apply to the Restricted Transfer and form part of this Addendum; or
- 6.3.2 in the absence of a separate signed data transfer appendix as provided for in paragraph 6.3.1 above, the data transfer appendix set out in the Appendix shall apply to the Restricted Transfer and form part of this Addendum,

and such relevant data transfer appendix will be the "DTA" for the purposes of this Addendum. Where there is any conflict between the terms of the Addendum and the terms of the DTA, the terms of the DTA will prevail to the extent of such conflict.

6.4 If, for whatever reason, the transfer of Personal Data under paragraph 6.3, is unlawful or ceases to be lawful:

- 6.4.1 you shall, on request by us, enter into a new data transfer appendix which implements Appropriate Safeguards as specified by us. Such new data transfer appendix will replace the DTA in paragraph 6.3.1 or 6.3.2 (as relevant) and on execution, shall be an appendix to, and form part of, this Addendum;
- 6.4.2 where Appropriate Safeguards have not been implemented in accordance with paragraph 6.4.1, we may cease any transfer of Personal Data.

7 Data Retention

- 7.1 We will not retain Personal Data for longer than is necessary to carry out any Permitted Data Purposes.
- 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 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.
- 8.3 We will act reasonably to keep you informed of ongoing developments in relation to any personal data breach involving Personal Data or otherwise in connection with the Services where required to do so by Data Protection Legislation.

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, joint controller or processor (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 adhere to ClearBank's Supplier Security Requirements (available on the Website at <https://www.clear.bank/legal>), as updated from time to time and also maintain adequate data processing, privacy and IT security policies in relation to your processing of personal data and any personal data breach or cyber security incident, that meet the requirements of Data Protection Legislation. You will comply with and procure that your Personnel comply, at all times with, such policies. You will ensure that your Personnel are subject to written confidentiality obligations which cover their processing of any personal data. Where specific control requirements are deemed by ClearBank to be not applicable to the Services, ClearBank may agree to waive or amend some of the requirements by notifying you of such waiver or amendment in writing;
 - 9.1.5 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 or which we otherwise process pursuant to the Agreement (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 Data Purposes 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 Data Purposes, 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 or set out in this Addendum) and such other information as required to be given by a controller to data subjects under the Data Protection Legislation;

- 9.1.6 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;
- 9.1.7 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;
- 9.1.8 you will ensure that any personal data you disclose or otherwise transfer to us is accurate;
- 9.1.9 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 Data Purposes and you will ensure that you delete from any documents that you disclose or transfer to us any such excessive or irrelevant personal data;
- 9.1.10 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 Personal Data or 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 Personal Data or 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;
- 9.1.11 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;

- 9.1.12 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
- 9.1.13 you warrant and represent that you have no reason to believe that the Data Protection Legislation prevents you from performing your obligations and exercising your rights under the Agreement; and
- 9.1.14 you will comply with any additional obligations imposed on you in the other applicable 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 Data Purposes 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 Data Purposes, 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 relating to Joint Data 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 Data Purposes 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 Data Purposes, 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, **Part 4 - Processor Terms** 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).
- 1.3 For the purposes of this **Part 4 - Processor Terms**, "Relevant Laws" shall mean as relevant:
 - 1.3.1 the laws of the United Kingdom (or any part of the United Kingdom) where the UK GDPR applies to the processing of Processor Data by us;
 - 1.3.2 the laws of Gibraltar where the Gibraltar GDPR applies to the processing Processor Data by us; or
 - 1.3.3 the laws of the EEA (or any member state of the EEA) where EU GDPR applies to the processing of Processor Data by us.

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 of the Processor Data 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 the Data Protection Legislation);

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

3.2.4 notifications to a 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 **Part 1 – General Terms**, 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 independent 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).

6 Reporting

6.1 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 involving Processor Data 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 you 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 involving Processor Data 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 (where permitted).

7 Using Sub-Processors

7.1 We will not engage a Sub-Processor to carry out any processing activities in respect of Processor Data on our behalf without your prior specific or general consent and subject to our compliance with paragraphs 7.2 and 7.3 of this **Part 4 – Processor Terms**.

7.2 We will:

7.2.1 ensure that there is a written contract in place with each Sub-Processor which requires the 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 Processor Data as those required under Article 28 GDPR including those set out in this **Part 4 – Processor Terms** and in applicable paragraphs in **Part 1 – General Terms**;

7.2.2 notify you of any Sub-Processor that we have not previously communicated to you (via our relevant policies or otherwise) by directing you to an updated list of (or otherwise). If you wish to object to the engagement of such new 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 7.2.1 of this **Part 4 – Processor 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 Sub-Processor we engage in the performance of its data processing obligations under the Agreement as if they were our own acts and omissions.

7.3 You consent to our use of the Sub-Processors set out in Schedule 1 of this Addendum, subject to our compliance with paragraph 7.2.1 of this **Part 4 – Processor Terms**.

Part 5 – Customer Processor Terms

Where you process personal data as a processor for ClearBank under or otherwise in connection with the Agreement (Protected Data), the provisions set out in this **Part 5 – Customer Processor Terms** will apply to the processing of Protected Data, in addition to Part 1 – General Terms. If a separate data processing addendum is signed by you and us, that will apply in place of this **Part 5**.

1 Instructions and Details of Processing

1.1 Insofar as you process Protected Data on behalf of ClearBank, you:

1.1.1 shall process the Protected Data for the purposes set out in Schedule 2 ("Permitted Data Purposes") and shall not process the Protected Data in a way that is incompatible with the Permitted Data Purposes;

1.1.2 unless required to do otherwise by Relevant Laws, shall (and shall take steps to ensure each person acting under your authority shall) process the Protected Data only on and in accordance with the Agreement, Schedule 2 and any other documented instructions from ClearBank (including with regard to any transfers to a third country or an international organisation) all as updated from time to time upon written agreement between the parties ("Processing Instructions"); and

1.1.3 if Relevant Laws require you to process Protected Data other than in accordance with the Processing Instructions, shall notify ClearBank of any such requirement before processing the Protected Data (unless Relevant Laws prohibit such information on important grounds of public interest).

1.2 For the purposes of this **Part 5– Customer Processor Terms**, "Relevant Laws" shall mean as relevant:

1.2.1 the laws of the United Kingdom (or any part of the United Kingdom) where the UK GDPR applies to the processing of Processor Data by us;

1.2.2 the laws of Gibraltar where the Gibraltar GDPR applies to the processing Processor Data by us; or

1.2.3 the laws of the EEA (or any member state of the EEA) where EU GDPR applies to the processing of Protected Data by you.

1.3 You shall notify us without delay if you become aware that any of the Protected Data is inaccurate or has become outdated.

2 Technical and Organisational Measures

2.1 You shall only provide the Protected Data to us by using secure methods as agreed and set out in Schedule 2.

2.2 You shall implement and maintain, at your own cost and expense, 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 Legislation and ensure the protection of the rights of data subjects;
 - 2.2.2 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; and
 - 2.2.3 assist us in responding to Data Subject Requests.
- 2.3 The level of technical and organisational measures agreed to by the parties as appropriate as at the Commencement Date having regard to the matters referred to in paragraph 2.2 are as set out in Schedule 2. The measures shall be regularly tested, assessed, and evaluated to assess their effectiveness for ensuring the security of the processing and you shall maintain records of such testing. The parties shall keep the measures under review and you shall carry out such updates as we reasonably deem appropriate.
- 2.4 You are responsible for ensuring that your Personnel involved in the processing of Protected Data are appropriately trained to handle and process the Protected Data in accordance with the ClearBank's Supplier Security Requirements (available on the Website at <https://www.clear.bank/legal>) as updated from time to time and with Data Protection Legislation. The level, content and regularity of training shall be proportionate to the Personnel's role, responsibility and frequency with respect to their handling and processing of the Protected Data. You will maintain, and regularly review, records of training undertaken by your personnel. At a minimum, all Personnel should receive annual training in relation to the GDPR and the processing of personal data.

3 Sub-Processors

- 3.1 You shall not engage a Sub-Processor to carry out any processing activities in respect of the Protected Data without our specific prior written consent and subject to compliance with paragraphs 3.2 and 3.3 and paragraph 5 below.
- 3.2 You shall:
- 3.2.1 provide details to us of any Sub-Processor;
 - 3.2.2 notify us 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 us to decide whether to consent to the change. We shall be entitled to object to any change in the Sub-Processor and at our 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 you fail to take the steps suggested by us to address the objection and otherwise do not cease to use the relevant Sub-Processor;
 - 3.2.3 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 **Part 5**, including an obligation on the Sub-Processor to provide sufficient guarantees to implement equivalent technical and organisational measures in accordance with paragraph 2 and to delete or return the Protected Data in accordance with paragraph 8. The contract with the Sub-Processor shall state that compliance with the obligations may be enforced by ClearBank including if you cease to exist or becomes insolvent. On request, you shall provide a copy of the contract with the Sub-Processor. You may redact the text of the contract to the extent necessary to protect confidential information including any personal data; and

- 3.2.4 notify us of any failure by a Sub-Processor to fulfil its contractual obligations referred to in paragraph 3.2.3.
- 3.3 You shall ensure that all persons authorised by you (or by any Sub-Processor) to process Protected Data are subject to an obligation to keep the Protected Data confidential. You shall grant access to the Protected Data to members of your Personnel on an "as needed basis" for the Permitted Data Purposes only.
- 3.4 You shall remain fully liable to us for any and all acts and omissions of any Sub-Processor, and any persons authorised by it (or by any Sub-Processor) to process Protected Data, as if they were your own.

4 Assistance and Data Subject Rights

- 4.1 You are responsible for maintaining a record of Data Subject Requests. Upon receipt of any Data Subject Request, you shall immediately (and no later than within 48 hours of receipt) refer such Data Subject Request to us and shall, at your own expense, promptly assist us with such Data Subject Request to ensure that we meet the response times under the Data Protection Legislation. You shall not respond to a Data Subject Request except on our documented instructions or as required by Relevant Laws, in which case you shall, to the extent permitted by Relevant Laws, inform us of that legal requirement prior to responding to such Data Subject Request.
- 4.2 You shall provide such assistance as reasonably required by us to ensure compliance with our obligations under the Data Protection Legislation with respect to:
 - 4.2.1 security of processing;
 - 4.2.2 data protection impact assessments (as such term is defined in the Data Protection Legislation);
 - 4.2.3 prior consultation with a Supervisory Authority regarding high risk processing;
 - 4.2.4 notifications to the Supervisory Authority and/or communications to data subjects by us in response to any personal data breach; and

- 4.2.5 any remedial action to be taken in response to a personal data breach and/or a Data Complaint or request relating to either party's obligations under the Data Protection Legislation relevant to the Agreement.

5 International Data Transfers

- 5.1 You shall not transfer, access or process Protected Data outside of the UK and the EEA without first having obtained our explicit written consent and, under no circumstances, prior to having in place Appropriate Safeguards agreed in writing with us.
- 5.2 To the extent that the transfer of any Protected Data between us and you pursuant to the Agreement is a Restricted Transfer, the provisions set out in **Part 1 – General Terms** paragraph 6.3 (Data Transfers) apply.

6 Records, Information and Audit

- 6.1 You shall maintain, in accordance with the Data Protection Legislation, complete and up to date written records of all categories of processing activities carried out on behalf of ClearBank.
- 6.2 You shall, in accordance with the Data Protection Legislation, promptly make available to us such information as we request from time to time, including any records under paragraph 6.1 and any information that is necessary to demonstrate your compliance with your obligations under this Addendum and the Data Protection Legislation. You shall immediately inform us if, in your reasonable opinion, an instruction infringes the Data Protection Legislation or any Relevant Laws.
- 6.3 Without prejudice to the above, we shall be entitled to (or mandate an independent auditor to) inspect, test and audit, all facilities, premises, equipment, systems, documents and electronic data relating to the processing of Protected Data by you to the extent such inspections and audits are necessary to demonstrate your compliance with your obligations under this Addendum (including where required by a Supervisory Authority). Such inspections and audits shall be at reasonable times and with prior written notice, subject to any inspection or audit required by a Supervisory Authority where this is not possible. You shall provide full cooperation and assistance in relation to such inspection, test and audit (subject to any confidentiality obligations) and on request shall provide copies of the results of any penetration and security testing procedures and third party audit reports such as SOC II reports (if such reports are available).
- 6.4 Without prejudice to our other rights and remedies, in the event that we identify any non-compliance with this Addendum as a result of an inspection, test or audit, you shall take such steps as we may reasonably request in order to promptly remedy the non-compliance, at no further cost to ClearBank.
- 6.5 We shall be entitled to share any records under paragraph 6.1, details, notification or information provided by or on behalf of you under the Addendum with any company within our Group, professional advisors and/or a Supervisory Authority.
- 6.6 You shall make any information referred to in this paragraph 6, including the results of any audit, available to the competent Supervisory Authority on request.

7 Breach Notification and Data Complaints

- 7.1 In respect of any personal data breach relating to, involving or affecting the Protected Data, you shall, without undue delay but in no event later than 24 hours (or earlier where possible) after becoming aware, notify us of the personal data breach and provide us 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 you to mitigate the effects of the personal data breach. Where, and insofar as, it is not possible for you to provide all of this information at the same time, the initial notification will provide such information as available to you and you shall provide the further information as soon as it becomes available without undue delay (but in no event later than 24 hours after it becomes available). If you become aware of a personal data breach in relation to the Protected Data, you will notify us by email at dataprotectionofficer@clear.bank.
- 7.2 You shall immediately, at your own expense, investigate any personal data breach relating to, involving or affecting the Protected Data and take steps to identify, prevent and mitigate the effects of and to remedy the same. You shall not release or publish any filing, communication, notice, press release or report concerning any such personal data breach without our prior written approval.
- 7.3 You shall promptly (but in no event later than 48 hours after becoming aware) inform us if you receive or become aware of a Data Complaint and shall not respond to the Data Complaint without our prior written approval.

8 Deletion or Return of Protected Data and Copies

- 8.1 You shall process the Protected Data only for the duration of the Agreement unless storage of any Processor Data is required by Relevant Laws, in which case you will be entitled to retain the same in accordance with Relevant Laws.
- 8.2 You shall ensure that any Protected Data (and all copies) are securely returned to us or destroyed (at our discretion and direction) in accordance with our instructions (unless storage is required by Relevant Laws and, if so, you shall inform us of any such requirement) in the following circumstances:
- 8.2.1 on termination of the Agreement;
 - 8.2.2 once processing of the Protected Data is no longer necessary for the Permitted Data Purposes; or
 - 8.2.3 otherwise at our request.
- 8.3 Following the destruction of the Protected Data in accordance with paragraph 8.2, you shall certify to us that the Protected Data in question has been destroyed in accordance with our instructions.

9 Warranties

- 9.1 You warrant and represent that:

- 9.1.1 your personnel, agents, Sub-Processors and any other person or persons accessing the Protected Data on your behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;
- 9.1.2 you and anyone operating on your behalf will process the Protected Data in compliance with the Data Protection Legislation;
- 9.1.3 you have ISAE3402 certification and you will maintain this certification for as long as you process the Protected Data.

10 Indemnity

- 10.1 You shall indemnify, and keep ClearBank fully and effectively indemnified, in respect of any and all losses, liabilities, damages, fines, penalties, sanctions, compensation, settlements, costs (including legal fees on an indemnity basis), interest, cost of compliance and expenses incurred by or awarded against or agreed to be paid by ClearBank arising from or in connection with any breach by you (or any Sub-Processor) of this Addendum and/or of the Data Protection Legislation.
- 10.2 Any exclusions and/or limitations of liability in the Agreement shall not apply your breach of this Addendum and/or the Data Protection Legislation, and/or to the indemnity in paragraph 10.1 of this Addendum.
- 10.3 You do not exclude or restrict your liability under this Addendum or the Data Protection Legislation on the basis that you have authorised a third party (including a Sub-Processor) to perform any of your obligations.

11 Non-Compliance

- 11.1 You shall inform us immediately if, at any time, you are unable to comply with your data protection obligations set out in this Addendum and/or in Data Protection Legislation.
- 11.2 If you are in breach of your obligations under this Addendum and/or Data Protection Legislation or have informed us of your inability to comply with your obligations pursuant to paragraph 11.1, we may (without liability) instruct you to suspend the processing of Protected Data until you rectify the non-compliance.
- 11.3 We shall be entitled, without liability, to terminate this Addendum and the Agreement (or that part of the Agreement that involves processing of Protected Data) if:
 - 11.3.1 the processing of Protected Data by you has been suspended by us pursuant to paragraph 11.2 and, if compliance with this Addendum and/or Data Protection Legislation is not restored within a reasonable time as determined by us at our discretion;
 - 11.3.2 you are in substantial or persistent breach of this Addendum; and/or
 - 11.3.3 you fail to comply with a binding decision of a competent court or Supervisory Authority regarding your obligations pursuant to this Addendum and/or under Data Protection Legislation.

11.4 Notwithstanding termination of the Agreement, this Addendum will remain in effect until you cease to process any Protected Data.

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 Data Purposes.
Duration of the Personal Data Processing/Retention Period	For the duration of the Agreement and for such time as required by Relevant Laws on a continuous basis.
The nature and purpose of the Personal Data Processing/Transfer	The processing of personal data in the provision of the Services by ClearBank to you as required for the Permitted Data Purposes.
The type of Personal Data	Personal data relating to individuals that is provided to ClearBank or otherwise obtained by ClearBank for the Permitted Data Purposes including identity data, contact data, financial data, transactional 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).
Sensitive Data	Special category data including details about race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about health and genetic and biometric data. Criminal conviction and offence data including data relating to terrorist offences and fraudulent activity.
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 a party processes in connection with the Services or in contemplation of the provision of services or otherwise for the Permitted Data Purposes including Clients, payers, and

	payees (all as further detailed in the Privacy Notice).
--	---

Part 2 - Approved Sub-Processors

Arkk Solutions

Compliancy Services Ltd

Diligent

DocuSign

Exela

Freshworks Inc.

Jaid

JP Morgan

Konica Minolta

LexisNexis Risk Solutions (UK) Ltd

Microsoft

Napier Technologies Limited

PagerDuty

Panorays

Regnology UK Limited

RingCentral UK Limited

Salesforce

Copado

ThetaRay Ltd

VERMEG

Other third parties as set out in the Privacy Notice - <https://clear.bank/privacy-notice>
(as updated from time to time)

**SCHEDULE 2
DATA PROCESSING DETAILS – PROTECTED DATA**

Detail	Description
Subject matter of the Personal Data Processing	The processing of personal data as required for the Permitted Data Purposes.
Duration of the Personal Data Processing/Retention Period	For the duration of the Agreement and for such time as required by Relevant Laws on a continuous basis.
The nature and purpose of the Personal Data Processing/Transfer	The processing of personal data in the provision of the Services as required for the Permitted Data Purposes.
The type of Personal Data	Personal data relating to individuals that is provided for the Permitted Data Purposes including identity data, contact data, financial data, transactional 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).
Sensitive Data	Special category data including details about race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about health and genetic and biometric data. Criminal conviction and offence data including data relating to terrorist offences and fraudulent activity.
The categories of Data Subject	Individuals about whom personal data is provided by or at ClearBank's direction in connection with the Services or in contemplation of the provision of services or otherwise for the Permitted Data Purposes including Clients, payers, and payees (all as further detailed in the Privacy Notice).

Appendix

DATA TRANSFER APPENDIX ("DTA")

The parties agree that, if you are located in a country or territory outside of the UK/Gibraltar/EEA which is not the subject of a relevant Adequacy Decision, there will be a Restricted Transfer if ClearBank transfers Personal Data to you. Such Restricted Transfer is subject to the terms of this DTA which sets out the Appropriate Safeguards for the Restricted Transfer as required under the GDPR unless we have entered into a separate data transfer appendix with you which is stated to replace this DTA. This DTA shall be deemed attached to and form part of the Addendum. Any provision of the Addendum that does not relate to a Restricted Transfer shall be unaffected by this DTA and shall remain in full force and effect.

1 DEFINITIONS AND INTERPRETATION

- 1.1 Terms used in this DTA shall have the meanings set out below, in the Addendum or as otherwise defined in the UK Addendum, Gibraltar Addendum or EU SCCs. Where a term is defined in both the Addendum and this DTA, the meaning of the term in this DTA shall have precedence in relation to this DTA. Where a term is defined in both this DTA, the UK Addendum, the Gibraltar Addendum or the EU SCCs, the meaning of the term in the UK Addendum, the Gibraltar Addendum or the EU SCCs (as applicable) shall have precedence in relation to the UK Addendum or the EU SCCs (as applicable).

"Adequacy Decision"	a valid adequacy decision or adequacy regulations pursuant to Article 45 of the EU GDPR or the UK GDPR (as appropriate);
"Appropriate Safeguards"	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 and the implementation of binding corporate rules pursuant to Article 47 GDPR;
"EU SCCs"	the standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council;
"EU GDPR"	the General Data Protection Regulation (EU) 2016/679;
"GDPR"	the UK GDPR, the Gibraltar GDPR or the EU GDPR (as applicable);
"Gibraltar GDPR"	has the meaning set out in section 2(1) of Gibraltar's Data Protection Act 2004;

"Gibraltar Addendum"	the template Addendum Version 1 issued by Gibraltar's Information Commissioner under s.128A(1) of the Gibraltar Data Protection Act 2004 on 7th December 2022;
"Mandatory Clauses"	the mandatory clauses in Part 2 of the UK Addendum or Gibraltar Addendum (as applicable);
"Restricted Transfer"	a transfer of personal data which is covered by Chapter V of the GDPR but which is not to a territory covered by an Adequacy Decision and which is made between the parties pursuant to or in connection with the Agreement;
"UK Addendum"	the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18;
"UK GDPR"	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

2 APPROPRIATE SAFEGUARDS

2.1 In the case of the Restricted Transfer, the Appropriate Safeguards that will apply depends upon whether the Restricted Transfer is governed by the UK GDPR, Gibraltar GDPR or the EU GDPR as follows:

2.1.1 **Restricted Transfer governed by the UK GDPR** - The UK Addendum (which incorporates the EU SCCs as amended in accordance with the Mandatory Clauses) applies and is incorporated into this DTA by reference and is deemed completed as follows:

2.1.1.1 Table 1 (Parties) - is completed with the information set out in Annex 1 of the DTA;

2.1.1.2 Table 2 (Selected SCCs, Modules and Clauses) – the EU SCCs apply including the information set out in Table 3 and with only the modules, clauses and optional provisions of the EU SCCs brought into effect for the purposes of the UK Addendum as set out in Annex 2 of the DTA. The module that will apply is as set out in paragraph 2.2 below;

2.1.1.3 Table 3 (Appendix Information) – the information which must be provided in the Appendix of the EU SCCs is as set out in Annex 3;

2.1.1.4 Table 4 (Ending the UK Addendum when the Approved Addendum Changes) – For the purposes of Section 19 of the Mandatory Clauses, only the Exporter identified in Annex 1 of the DTA may end the UK Addendum.

2.1.2 **Restricted Transfer governed by the Gibraltar GDPR** – The Gibraltar Addendum (which incorporates the EU SCCs as amended in accordance

with the Mandatory Clauses) applies and is incorporated into this DTA by reference and is deemed completed as follows:

- 2.1.2.1 Table 1 (Parties) - is completed with the information set out in Annex 1 of the DTA;
- 2.1.2.2 Table 2 (Selected SCCs, Modules and Clauses) – the EU SCCs apply including the information set out in Table 3 and with only the modules, clauses and optional provisions of the EU SCCs brought into effect for the purposes of the Gibraltar Addendum as set out in Annex 2 of the DTA. The module that will apply is as set out in paragraph 2.2 below;
- 2.1.2.3 Table 3 (Appendix Information) – the information which must be provided in the Appendix of the EU SCCs is as set out in Annex 3;
- 2.1.2.4 Table 4 (Ending the Gibraltar Addendum when the Approved Addendum Changes) – For the purposes of Section 19 of the Mandatory Clauses, only the Exporter identified in Annex 1 of the DTA may end the Gibraltar Addendum.

2.1.3 **Restricted Transfer governed by the EU GDPR** – The EU SCCs apply and are incorporated into this DTA by reference and deemed completed as follows:

- 2.1.3.1 The modules, clauses and optional provisions are as set out in Annex 2 of the DTA. The module that will apply is as set out in paragraph 2.2 below.
- 2.1.3.2 Clause 17 – Option 1 will apply and the EU SCCs will be governed by the law of the Republic of Ireland.
- 2.1.3.3 Clause 18(b) – Disputes will be resolved before the courts in the Republic of Ireland.
- 2.1.3.4 Appendix - The information which must be provided in the Appendix of the EU SCCs is as set out in Annex 3 of the DTA.

2.2 The modules of the EU SCCs that will apply for the purposes of paragraphs 2.1.1, 2.1.2 and 2.1.3 shall be as follows:

- 2.2.1 Module One (Controller to Controller) – shall apply where we process Personal Data as a joint controller or an independent controller and transfer Personal Data to you, acting as a joint controller or an independent controller;
- 2.2.2 Module Two (Controller to Processor) – shall apply where you process Protected Data as a processor for us acting as a controller;
- 2.2.3 Module Four (Processor to Controller) – shall apply where we process Personal Data as a processor and transfer Personal Data to you, acting as a controller.

3 CONFLICTS

- 3.1 It is not the intention of either party to contradict or restrict any of the provisions set out in the UK Addendum, Gibraltar Addendum or the EU SCCs and, accordingly, if and to the extent that, any provision of the Agreement conflicts with the UK Addendum, Gibraltar Addendum or the EU SCCs, then the UK Addendum, Gibraltar Addendum or EU SCCs (as applicable) will prevail to the extent of such conflict.

4 SIGNATURE OF THE UK ADDENDUM, GIBRALTAR ADDENDUM AND EU SCCS

- 4.1 By signing the Agreement, the parties are deemed to have signed the UK Addendum, Gibraltar Addendum and Annex 1A of the EU SCCs (as applicable) without any further signature from either party.

ANNEX 1 OF THE DTA
PARTIES

THIS TABLE MUST BE COMPLETED WHEN THE DSA IS SIGNED

The Parties	Exporter/data exporter (who sends the Restricted Transfer)	Importer/data importer (who receives the Restricted Transfer)
Parties Details	Name: ClearBank Limited Address: Borough Yards, 13 Dirty Lane, London, SE1 9PA Company No: 09736376	Name: As set out in the Agreement Address: As set out in the Agreement Company No: As set out in the Agreement
Key Contact	Position: DPO Email: DataProtectionOfficer@clear.bank	Name: As set out in the Agreement or provided to the Exporter Position: As set out in the Agreement or provided to the Exporter Email: As set out in the Agreement or provided to the Exporter
Activities relevant to the data transferred	Modules One and Four - As set out in Schedule 1 Part 1 – Data Processing Details of the Addendum. Module Two – As set out in Schedule 2 – Data Processing Details of the Addendum.	Modules One and Four - As set out in Schedule 1 Part 1 – Data Processing Details of the Addendum. Module Two – As set out in Schedule 2 – Data Processing Details of the Addendum.
Role	As determined in accordance with paragraph 2.2 of the DTA	As determined in accordance with paragraph 2.2 of the DTA
Transfer details	From the UK	To the location of the Importer

**ANNEX 2 OF THE DTA
SELECTED MODULES AND CLAUSES**

The following modules, clauses or optional provisions of the EU SCCs shall apply:

Module	Clause 7 (Docking Clause)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time Period)	Clause 11 (Option)	Is personal data received from the Importer combined with personal data collected by the Exporter
One (Controller to Controller)	Will not apply	Not Applicable	Not Applicable	The optional language will not apply	Not Applicable
Two (Controller to Processor)	Will not apply	Option 1 Specific Prior Authorisation will apply	30 days	The optional language will not apply	Not Applicable
Four (Processor to Controller)	Will not apply	Not Applicable	Not Applicable	The optional language will not apply	Where required under the Agreement.

**ANNEX 3 OF THE DTA
ANNEXES**

The Annexes in the Appendix of the EU SCCs shall be deemed completed as follows:

Annex 1A	UK GDPR or GIBRALTAR GDPR	EU GDPR
The Parties	As set out in Annex 1.	
Annex 1B	UK GDPR or GIBRALTAR GDPR	EU GDPR
Description of Transfer	<p>Categories of data subject: As set out in Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details of the Addendum</p> <p>Categories of personal data: As set out in Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details of the Addendum</p> <p>Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved: As set out in Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details of the Addendum</p> <p>Frequency of transfer: Continuous</p> <p>Nature of processing: As set out in Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details of the Addendum</p> <p>Purpose of data transfer and further processing: As set out in Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details of the Addendum</p> <p>Retention period: As set out in Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details of the Addendum</p>	
Annex 1C	UK GDPR or GIBRALTAR GDPR	EU GDPR
Competent Supervisory Authority (Module One and Two only)	Not used. See Mandatory Clauses in UK Addendum.	Irish Data Protection Commissioner
Annex II	UK GDPR or GIBRALTAR GDPR	EU GDPR
Technical and Organisational Measures Including Technical and Organisational	As set out in Part 1 – General Terms of the UK Addendum or Gibraltar Addendum (as applicable)	

Measures to ensure the Security of the Data (Module One only)		
Annex III	UK GDPR or GIBRALTAR GDPR	EU GDPR
List of Sub Processors	Not Applicable for Module One or Four Module Two – To be discussed and agreed by the parties on a case by case basis.	