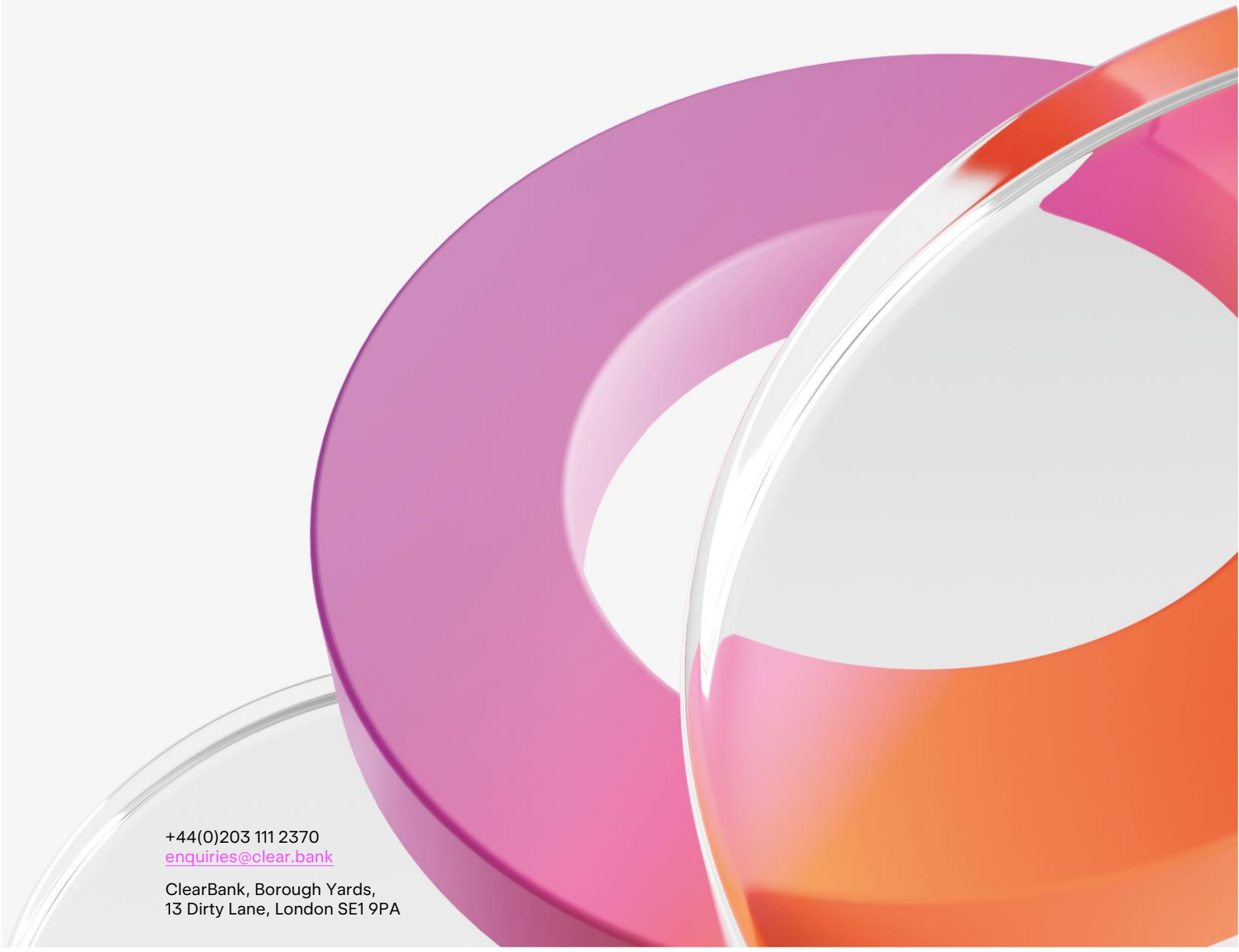
Clear.Bank

Client Terms

Data Protection Addendum



+44(0)203 111 2370
enquiries@clear.bank

ClearBank, Borough Yards,
13 Dirty Lane, London SE1 9PA

Clear.Bank

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 referenced above which incorporates this Addendum;
"Agreement Data"	means any and all personal data that is processed by either party pursuant to or in connection with the Agreement irrespective of its Processing Role, including Processor Data (as the context requires);
"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;
"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 (but does not include a Data Subject Request);
"Data Controller"	has the meaning given to that term in Part 2;
"Data Processor"	has the meaning given to that term in Part 2;
"Data Protection Legislation"	means any applicable laws and regulations in the UK relating to privacy and/or the processing of personal data and applicable to a party including: (a) the Data Protection Act 2018 and the UK GDPR; (b) the Gibraltar GDPR and the Data Protection Act 2004;

	(c) the EU GDPR; and (d) 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, each as updated, replaced, extended or amended from time to time;
"Data Subject Request"	means a request made by a data subject to exercise any of its rights as a data subject under the Data Protection Legislation relating to its personal data;
"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 paragraph 5.3 of Part 1 and which sets out the Appropriate Safeguards for a Restricted Transfer;
"EEA"	means the member states of the European Economic Area;
"EU GDPR"	means Regulation (EU) 2016/679 of the European Council of 27 April 2016;
"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 *subsidiary* and *holding company* are as defined in section 1159 of the Companies Act 2006*;*
"Insolvency Event"	means, in relation to a party, that the party: (i) is unable, or admits inability, to pay its debts within the meaning of section 123 of the Insolvency Act 1986 or suspends or threatens to suspend making a payment on any of its debts; (ii) has an order made against it or a resolution passed for its administration, winding-up or dissolution or any other corporate step or legal proceeding is taken with a view to the same (otherwise than for the purposes of a solvent amalgamation or reconstruction); (iii) has an administrative receiver, receiver, manager, liquidator, administrator, trustee or similar officer appointed over all or any substantial part of its assets;

	(iv) enters into or proposes any compromise, composition or arrangement with its creditors generally; (v) is granted a moratorium or similar relief under applicable insolvency laws, allowing temporary suspension of debt obligations to facilitate restructuring efforts; or (vi) suffers or carries out anything analogous to the foregoing in any applicable jurisdiction;
"Permitted Data Purposes"	has the meaning given to that term in paragraph 1.1 of Part 1 or means such purposes as set out in the Agreement (as applicable);
"Personnel"	means, in respect of a party or a member of its Group, their directors, officers, employees, consultants, agents 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 Website and which may be updated from time to time by ClearBank;
"Processing Role"	has the meaning given to that term in paragraph 2.1 of this Addendum;
"Processor Data"	has the meaning given to that term in Part 2;
"Records"	means accurate, complete, and up to date records of a party's processing activities relating to Agreement 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 UK, or any other relevant jurisdiction, which are applicable to this Agreement (including Data Protection Legislation, 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 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;
"Regulatory Authority"	means any 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;
"Security Breach"	means any actual loss, unauthorised or unlawful processing, destruction, damage, or alteration, or unauthorised disclosure of, or access to Agreement Data;
"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 UK's Information Commissioner 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);
"UK GDPR"	has the meaning set out in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018; 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 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", and unless this Addendum expressly provides otherwise, each of those persons will be jointly and severally liable for each of the obligations and liabilities

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 Processing Roles

2.1 In providing or receiving the Services and otherwise complying with its obligations under the Agreement, either party may act as a joint controller, a controller, or a processor of personal data respectively (each, a "**Processing Role**").

2.2 In respect of Services provided under the Agreement, we have determined the Processing Roles as indicated in the table below, which apply unless you inform and agree with us otherwise in writing:

Service	ClearBank's Processing Role	Customer's Processing Role
Transactional and agency banking (excluding CoP aggregator services)	Independent Controller	Independent Controller
CoP aggregator services	Processor	Controller
Embedded banking	Controller	Processor
Corporate banking	Independent Controller	Independent Controller

2.3 Where a provision of this Addendum applies to a party where it has a specific Processing Role, such provision applies only in respect of Agreement Data for which that party has such Processing Role and only to the extent it is processing Agreement Data.

2.4 This Addendum is divided into the following parts:

(a) Part 1 - General Terms (**Part 1**) – these terms apply irrespective of either party's Processing Role;

(b) Part 2 - Processor Terms (**Part 2**) – these terms apply only where one party acts as a processor for the other party acting as a controller.

2.5 If there is any conflict between the provisions in Part 1 and the provisions in Part 2, then the provisions in Part 2 will prevail to the extent of the conflict.

Clear.Bank

Part 1

General Terms

1 Data Processing

1.1 The parties may process Agreement Data solely:

(a) as required in the provision or receipt (as applicable) of the Services;

(b) for the performance and exercise of that party's rights and obligations under the Agreement; and

(c) in ClearBank's case only, in contemplation of the provision of any services by us, for verification, fraud and crime prevention, 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, (collectively, the "**Permitted Data Purposes**").

1.2 Where we are processing Agreement Data, we will do so in accordance with Schedule 1 (as updated from time to time).

1.3 Each party will comply at all times with its obligations under the Data Protection Legislation in respect of such Agreement Data.

1.4 Each party will, where it acts as a controller in respect of Agreement Data:

(a) provide all necessary, fair and transparent information and notices to, and obtain all necessary consents from, any data subjects whose Agreement Data it provides to the other party under or in connection with the Agreement (including Personnel and, in the Customer's case, Direct Third Party Service Providers and Clients) and ensure that such information and notices details: (i) the processing of such Agreement Data as required for the Permitted Data Purposes, (ii) the legal basis for such processing, (iii) the recipients of Agreement Data (including Relevant Payment System Operators and Regulatory Authorities) and (iv) such other information as required to be given by a controller to data subjects under the Data Protection Legislation; such that the other party is lawfully able to use or process such Agreement Data for the Permitted Data Purposes without needing further consent, approval or authorisation and, if requested by the other party, promptly provide reasonable evidence to that party that it has obtained all such necessary consents and otherwise complied with its obligations under the Data Protection Legislation; and

(b) maintain any valid registrations and pay any fees as required by its national Supervisory Authority to cover its processing activities contemplated for the Permitted Data Purposes.

1.5 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 While Agreement Data is within its possession or control, each party will maintain, appropriate technical and organisational measures and policies to:

(a) ensure the security, integrity, availability and confidentiality of Agreement Data; and

(b) protect against unauthorised or unlawful processing of Agreement Data and the accidental loss or destruction of, or damage to, Agreement Data, such measures to be appropriate to (i) the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction of, or damage to, Agreement Data and (ii) the nature of the data to be protected, in each case having regard to the state of technological development and the cost of implementing any measures. Each party also procures that its Personnel shall comply, at all times, with such measures and policies.

2.2 We have the following security measures in place:

(a) **Access Controls** – access to Agreement 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;

(b) **Encryption** – encryption of Agreement Data at rest and in transit;

(c) **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;

(d) **Mutual Authentication** – use of mTLS authentication;

(e) **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

(f) **Data Backup** – data is backed up according to an agreed backup schedule.

2.3 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.

2.4 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 will ensure that the external party will on request, provide you with a summary of any conclusions drawn or recommendations made following such review or audit. 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 you become aware of any potential vulnerability in relation to our technical and organisational measures referred to in paragraph 2.1 of this Part 1, you will promptly advise us about such potential vulnerability and we will take all reasonable steps necessary, in our opinion, to mitigate or remove such vulnerability and keep you informed of all such progress.

3 Staff and Training

3.1 Each party will ensure that its Personnel are appropriately trained to process Agreement Data in accordance with the Data Protection Legislation and this Addendum. 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 Agreement Data. Each party will maintain, and regularly review, records of training undertaken by its Personnel. At a minimum, all staff of either party will receive annual training in relation to the Data Protection Legislation and the processing of personal data.

3.2 Each party will ensure that all persons authorised by it (or by any processor or Sub-Processor) to process Agreement Data (including Personnel) are subject to an obligation to keep Agreement Data confidential.

4 Records

4.1 Each party will, having regard to its Processing Role in respect of Agreement Data, document and maintain its Records to the extent required to comply with Data Protection Legislation and this Addendum in respect of such Agreement Data, and to the extent reasonably necessary to demonstrate such compliance, except to the extent prohibited by Relevant Law, make available such Records to the other party upon reasonable request.

4.2 Each party will ensure that all Records and other information obtained by it or its auditor under or in connection with this paragraph 4 of this Part 1, are kept strictly confidential and it will not disclose the same to a third party unless required to do so by a Regulatory Authority, in which case, it will (to the extent legally permissible and reasonably practicable) give the other party written notice of such requirement.

5 Data Transfers

5.1 We will not transfer Agreement Data to a country or territory outside of the United Kingdom, Gibraltar or the EEA including to a Sub-Processor located in such a country or territory unless:

(a) there is an Adequacy Decision in respect of that country or territory; or

(b) 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

(c) 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.

5.2 If, for whatever reason, the transfer of Agreement Data pursuant to paragraph 5.1 of this Part 1 ceases to be lawful, we will immediately implement other Appropriate Safeguards and ensure that the level of protection afforded to Agreement Data in the destination country or territory is equivalent to the level of protection that would be afforded to Agreement Data in the UK, Gibraltar or the EEA (as applicable to the transfer) under the Data Protection Legislation. Where we cannot do that, we will cease any such transfer of Agreement Data.

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

(a) 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 will apply to the Restricted Transfer and form part of this Addendum; or

(b) in the absence of a separate signed data transfer appendix as provided for in paragraph 5.3(a) of this Part 1, the data transfer appendix set out in the Appendix will 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.

5.4 If, for whatever reason, the transfer of Agreement Data under paragraph 5.3 of this Part 1, is unlawful or ceases to be lawful:

(a) you will, 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 on execution, be an appendix to, and form part of, this Addendum and replace the DTA;

(b) where Appropriate Safeguards have not been implemented in accordance with paragraph 5.4(a) of this Part 1, we may cease any transfer of Agreement Data.

6 Security Breaches

6.1 Either party will promptly (and in any event within 48 hours) notify the other party if it becomes aware of a Security Breach, such notice to include details of the Security Breach including the nature of the personal data breach, the categories and approximate volume of data subjects, the Agreement Data records concerned, the likely consequences of the Security Breach and any measures taken or to be taken to mitigate the effects of the Security Breach. Where you are notifying party, you will notify us by email at dataprotectionofficer@clear.bank.

6.2 Each party will provide reasonable co-operation and assistance to the other party as is necessary to facilitate the handling of the Security Breach in an expeditious and compliant manner and to enable the other party to comply with its obligations under the Data Protection Legislation.

6.3 Neither party will release or publish any filing, communication, notice, press release or report concerning any Security Breach unless required to do so under the Data Protection Legislation and/or by a Supervisory Authority, in which case it will notify the other party in advance of such requirement (where permitted).

6.4 The party suffering the Security Breach will take prompt action to investigate any Security Breach involving Agreement Data and to identify, prevent and mitigate the effects of and to remedy any such Security Breach.

6.5 Each party will act reasonably to keep the other party informed of ongoing developments in relation to any Security Breach.

7 Obligations

7.1 Irrespective of either party's Processing Role, each party:

(a) will be solely responsible for making an independent determination as to whether the technical and organisational measures implemented by the other party are adequate and meet the requirements of the Data Protection Legislation and any other obligations the party has under Relevant Laws;

(b) will be entitled to assume that any disclosure or transfer of personal data to the other party (directly or indirectly) is done so in a manner which is compliant with the Data Protection Legislation;

(c) will ensure that any personal data which it discloses or otherwise transfers to the other party is accurate;

(d) will not disclose or transfer to the other party, any excessive or irrelevant personal data that is not required by the other party in connection with the performance of the Services or otherwise for the Permitted Data Purposes and will ensure that it deletes from any documents that it discloses or transfers to the other party any such excessive or irrelevant personal data;

(e) will provide the other party with reasonable co-operation and assistance as may be required from time to time to enable the other party to comply with their 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;

(f) warrants and represents that it has no reason to believe that the Data Protection Legislation prevents it from performing its obligations and exercising its rights under the Agreement; and

(g) will comply with any additional obligations imposed on it in the other applicable Parts of this Addendum.

7.2 If you receive or become aware of a Data Subject Request or a Data Complaint, you will notify us promptly (to the extent legally permissible and within no more than 2 Business Days from such receipt or awareness) by email at dataprotectionofficer@clear.bank and you will provide reasonable co-operation and assistance to us as is necessary to deal with any such Data Subject Request or Data Complaint, except to the extent the Data Subject Request or Data Complaint relates to Processor Data, in which case Part 2 shall apply.

Clear.Bank

Part 2

Processor Terms

Where, in respect of the processing of Agreement Data, either party's Processing Role is as a processor ("**Data Processor**") for the other party ("**Data Controller**"), the provisions set out in this Part 2 will apply to such processing of such Agreement Data ("**Processor Data**") in addition to the provisions in Part 1, unless otherwise specified in this Part 2.

1 Instructions and Details of Processing

1.1 In performing its obligations as a processor, the Data Processor will, unless required to do otherwise by Relevant Laws, process the Processor Data only on and in accordance with the Agreement (including Part 1 and this Part 2) and any other documented instructions from the Data Controller (each as updated from time to time in accordance with the Agreement) solely for the Permitted Data Purposes.

1.2 If Relevant Laws require the Data Processor to process Processor Data other than in accordance with paragraph 1.1 of this Part 2, the Data Processor will notify Data Controller of any such requirement before processing the Processor Data, except to the extent prohibited by Relevant Law.

1.3 Where you are the Data Processor you will process Processor Data solely in accordance with Schedule 2.

1.4 The Data Processor will notify the Data Controller without delay if it becomes aware that any of the Processor Data is inaccurate or has become outdated.

2 Technical and Organisational Measures

2.1 The Data Processor will implement and maintain appropriate technical and organisational measures to:

(a) ensure its processing of Processor Data meets the requirements of the Data Protection Legislation (including Article 32 GDPR) and ensure the protection of the rights of data subjects, in each case including by complying with its obligations in paragraph 2 of Part 1; and

(b) provide reasonable assistance to the Data Controller in responding to Data Subject Requests relating to Processor Data.

2.2 Where you are the Data Processor, the level of technical and organisational measures agreed to by the parties in respect of your processing of Processor Data as appropriate as at the Commencement Date having regard to the matters referred to in paragraph 2.1 of Part 1 are as set out in Schedule 2. The measures will be regularly tested, assessed, and evaluated to assess their effectiveness for ensuring the security of the processing and you will maintain records of such testing. The parties will keep the measures under review and you will carry out such updates as we reasonably deem appropriate.

2.3 You will grant access to Processor Data to members of your Personnel on an "as needed basis" for the Permitted Data Purposes only.

3 Assistance and Data Subject Rights

3.1 If the Data Processor receives a Data Subject Request relating to the processing of Processor Data then, to the extent legally permissible, the Data Processor will as soon as reasonably practicable notify the Data Controller (and in any event within 2 Business Days of receipt of the Data Subject Request) and will provide reasonable co-operation and assistance to the Data Controller in executing its obligations under the Data Protection Legislation in relation to such Data Subject Request.

3.2 The Data Processor will not respond to a Data Subject Request except on the Data Controller's documented instructions or as required by Relevant Laws, in which case the Data Processor will, to the extent permitted by Relevant Laws, inform the Data Controller of that legal requirement prior to responding to such Data Subject Request.

3.3 The Data Processor will provide such assistance as the Data Controller reasonably requires in respect of complying with its obligations under the Data Protection Legislation with respect to:

(a) security of processing;

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

(c) prior consultation with a Supervisory Authority regarding high risk processing;

(d) notifications to a Supervisory Authority and/or communications to data subjects by the Data Controller in response to any personal data breach; and

(e) any remedial action to be taken in response to a Security Breach.

4 International Data Transfers

4.1 Where you are the Data Processor you will not transfer, access or process Processor 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 Information and Audit

5.1 Subject to paragraph 5.3 of this Part 2, the Data Processor will, in accordance with the Data Protection Legislation and as is reasonably necessary to demonstrate its compliance with its obligations as Data Processor under this Addendum and the Data Protection Legislation, allow for and contribute to audits, including inspections, by the Data Controller (or an independent auditor mandated by the Data Controller and agreed by the Data Processor in writing).

5.2 The Data Controller will:

(a) take into account the Data Processor's security certifications (including in our case those set out in paragraph 2 of Part 1) when deciding whether to carry out a review or audit;

(b) provide the Data Processor with reasonable prior written notice (not less than 10 Business Days) of any information request, audit and/or inspection that it requires;

(c) ensure that the Records and all information obtained or generated by the Data Controller or its auditor under or in connection with this paragraph 5 of this Part 2, are kept strictly confidential, and will not disclose the same to a third party unless required to do so by a Regulatory Authority, in which case, it will (to the extent legally permissible) not less than 14 days before such disclosure give prior written notice of such requirement to the Data Processor;

(d) ensure that such audit or inspection is undertaken during the Data Processor's normal business hours, with minimal disruption to its business and the business of its other customers;

(e) pay the Data Processor's reasonably incurred costs for assisting with, allowing for and contributing to such inspections and audits; and

(f) comply with any reasonable additional obligations which the Data Processor requires in relation to access by the Data Controller or its auditor, including in our case any security policies notified by us to you or as set out in the Agreement.

5.3 Nothing in paragraph 5 of this Part 2, gives the Data Controller the right to access any data of any of the Data Processors other customers, or any information that by permitting such access could cause the Data Processor to breach its obligations under Relevant Laws (including the Data Protection Legislation) or its confidentiality obligations owed to a third party.

5.4 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 undertaken under paragraph 5.1 above, you will take such steps as we may reasonably request in order to promptly remedy the non-compliance, at no further cost to ClearBank

6 Deletion or Return of Processor Data and Copies

6.1 The Data Processor will process the Processor Data only for as long as necessary to carry out any Permitted Data Purposes and only for the duration of the Agreement unless retention of any Processor Data is required by Relevant Laws, in which case the Data Processor will be entitled to retain such Processor Data to such extent required.

6.2 The Data Processor will maintain and comply with its data retention policy, details of which it will provide to the Data Controller on written request.

6.3 On termination of the Agreement, and at the Data Controller's written request, the Data Processor will return any Processor Data to the Data Controller or, at its option, securely destroy it to the extent reasonably practicable (unless retention of any Processor Data is required by Relevant Laws, in which case the Data Controller will be entitled to retain the same in accordance with Relevant Laws).

6.4 Following the destruction of the Processor Data in accordance with paragraph 6.3 the Data Processor will certify to the Data Controller on request that the Processor Data in question has been destroyed in accordance with its instructions.

7 ClearBank Sub-Processors

7.1 This paragraph 7 applies where we are the Data Processor.

7.2 You generally agree and consent to our engagement and appointment of the Sub-Processors set out in Schedule 1.

7.3 We will:

(a) ensure there is a written contract in place with each Sub-Processor requiring such Sub-Processor to only carry out such processing of Processor Data as may be necessary from time to time 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 set out in this Part 2 and in relevant paragraphs in Part 1; and

(b) notify you where we engage a Sub-Processor to process Processor Data which is not set out in Schedule 1, or that we have not previously communicated to you (via our relevant policies or otherwise) by directing you to an updated list of Sub-Processors (or otherwise). If you wish to object to such engagement you must provide us with written notice of such objection including reasonable details of the grounds for your objection as soon as possible and in any event with 10 days of receipt of our notice. Following our receipt of such notice, we will endeavour to discuss any reasonable objections with you in good faith. If, after 61 days from the date we received such notice, you can demonstrate that we have failed to comply with paragraph 7.3(a) of this Part 2, 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.

7.4 We will be responsible for the acts and omissions of any Sub-Processor we engage in respect of its processing of Processor Data in connection with the Agreement as if they were our own acts and omissions.

8 Customer Sub-Processors

8.1 This paragraph 8 applies where you are the Data Processor.

8.2 You will not engage a Sub-Processor to carry out any processing activities in respect of the Processor Data without our specific prior written consent and subject to your compliance with paragraphs 4 and 8 of this Part 2.

8.3 You will:

(a) provide details to us of any Sub-Processor;

(b) notify us 30 days in advance of any change in a Sub-Processor (through the addition or replacement of a Sub-Processor) and will provide such information as reasonably necessary to enable us to decide whether to consent to the change. We will 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 Processor 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;

(c) prior to the relevant Sub-Processor carrying out any processing activities in respect of the Processor Data, ensure there is a written contract in place with such Sub-Processor which (i) requires such Sub-Processor to only carry out such processing as may be necessary from time to time to perform one or more of your obligations 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 set out in this Part 2 and in applicable paragraphs in Part 1; (ii) states that ClearBank may enforce Sub-Processor's compliance with its obligations under the contract, including if you are subject to an Insolvency Event; and

(d) notify us of any failure by a Sub-Processor to fulfil its contractual obligations referred to in paragraph 8.3(c) of this Part 2.

8.4 You will remain fully liable to us for any and all acts and omissions of any Sub-Processor, and any persons authorised by it to process Processor Data, as if they were your own.

9 Warranties

9.1 You warrant and represent that:

(a) your Personnel, Sub-Processors and any other person or persons accessing Processor Data on your behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) you and anyone operating on your behalf will process Processor Data in compliance with the Data Protection Legislation; and

(c) you have ISAE3402 certification and you will maintain this certification for as long as you process the Processor 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 Part 2.

11 Non-Compliance

11.1 You will 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 as Data Processor 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 of this Part 2, we may (without liability) instruct you to suspend the processing of Processor Data until you rectify the non-compliance.

11.3 Where you are Data Processor, we will be entitled, without liability, to terminate this Addendum and the Agreement (or that part of the Agreement that involves your processing of Processor Data) if:

(a) the processing of Processor Data by you has been suspended by us pursuant to paragraph 11.2 of this Part 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;

(b) you are in substantial or persistent breach of this Addendum; and/or

(c) 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 Processor Data.

Clear.Bank

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

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

Clear.Bank

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 Agreement 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:

(a) **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:

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

(ii) 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;

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

(iv) 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.

(b) **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:

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

(ii) 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;

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

(iv) 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.

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

(i) 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.

(ii) Clause 17 – Option 1 will apply and the EU SCCs will be governed by the law of the Republic of Ireland.

(iii) Clause 18(b) – Disputes will be resolved before the courts in the Republic of Ireland.

(iv) 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 (a), (b) and (c) shall be as follows:

(a) Module One (Controller to Controller) – shall apply where we process Agreement Data as a joint controller or an independent controller and transfer Agreement Data to you, acting as a joint controller or an independent controller;

(b) Module Two (Controller to Processor) – shall apply where you process Processor Data as a **processor** for us acting as a controller;

(c) Module Four (Processor to Controller) – shall apply where we process Processor Data as a **processor** and transfer Agreement 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.

Clear.Bank

Annex 1 of the DTA

Parties

THIS TABLE MUST BE COMPLETED WHEN THE DTA 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

Clear.Bank

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.

Clear.Bank

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	Categories of data subject: As set out in **Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details** of the Addendum Categories of personal data: As set out in **Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details** of the Addendum 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 Frequency of transfer: Continuous Nature of processing: As set out in **Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details** of the Addendum 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 Retention period: As set out in **Schedule 1 or Schedule 2 (Module Two) Part 1 – Data Processing Details** of the Addendum	
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 Measures to ensure the Security of the Data (Module One only)	As set out in **Part 1 – General Terms** of the UK Addendum or Gibraltar Addendum (as applicable)	
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.	