Data Processing Addendum

19 August 2025

DATA PROCESSING ADDENDUM

This addendum (**Addendum**) supplements the IFX Corporate ibanq Terms and Conditions and the IFX Trading Terms and Conditions (Corporate), each as updated or amended from time to time and/or any such other agreement as is in place between the Client and IFX governing the use of the Services (together the **Agreement**).

This Addendum applies to Clients who are in receipt of our Services and shall become effective upon the Client receiving or agreeing to receive all or any of the Services. Should any member of the Client's Group receive or benefit from the Services, it is the Client's responsibility to ensure that the Client's Group company complies with this Addendum.

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

This Addendum is divided into the following parts:

(i) **Part 1 (General Terms)** – these terms apply irrespective of our role;

(ii) **Part 2 (Controller Terms)** – these terms apply where we act as an independent controller;

(iii) **Part 3 (Joint Controller Terms)** – these terms apply where we act as a joint controller; and

(iv) **Part 4 (Processor Terms)** – these terms apply where we act as a processor.

If there is any conflict between (i) the provisions in Part 1; and (ii) the provisions in any of Part 2, Part 3, or Part 4, the provisions in Part 2, Part 3 or Part 4 (as applicable) will prevail. In the event of any conflict between this Addendum and the other provisions of the Agreement, or the Privacy Notice, this Addendum will prevail.

1. Interpretation

1.1. The following definitions and rules of interpretation apply in this Addendum:

Appropriate Safeguards: means any legally enforceable mechanisms for transferring personal data permitted under the Data Protection Legislation, which may include those described in Article 46 of the GDPR and the implementation of binding corporate rules pursuant to Article 47 of the GDPR.

Business Day: means a day (other than a Saturday or Sunday or a public holiday) when banks are open for the transaction of normal banking business in London, United Kingdom.

Client, you: means the person(s) receiving any of the Services from IFX pursuant to the Agreement, or the end user who will use or benefit from the Services.

Commencement Date: means the effective date of the Agreement.

Controller Data: has the meaning given to that term in Part 2 of this Addendum.

Data Complaint: refers to any request or complaint regarding either party's obligations under the Data Protection Legislation, which includes complaints by data subjects or any notice, investigation, or action taken by a Supervisory Authority.

Data Protection Legislation: means (i) any legislation in force from time to time regarding the processing of personal data and privacy, including the UK Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 (GDPR), the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), and any laws or regulations implementing the Privacy and Electronic Communications Directive 2002/58/EC; (ii) any laws that replace, extend, re-enact, consolidate, or amend any of the aforementioned, whether before or after the date of the Agreement, from the date they come into force (except, if applicable domestic law permits, to the extent that the GDPR is modified by applicable domestic law from time to time, but where such modification deprives data subjects of their rights, which they would otherwise be entitled to if any relevant processing were carried out in the EEA, such modification will not affect this Agreement); and (iii) guidance and codes of practice issued by any relevant EEA Supervisory Authority that applies to a party.

Data Subject Request: means a request made by a data subject to exercise their rights under the Data Protection Legislation.

Direct Third-Party Service: means any service (or parts thereof) that is not provided by us under the Agreement but is wholly provided by a third-party provider. You 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 provider, including a TPP, that provides Direct Third-Party Services and with whom you will enter into a direct agreement in respect of those services.

EEA: means the European Economic Area.

GDPR: refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Group: means in relation to a company, that company, any subsidiary or any holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company. Each company in a Group is a member of the Group.

IFX, we, or us: means IFX (UK) Ltd, incorporated and registered in England and Wales with company registration number 05422718, trading as IFX Payments.

Joint Data: has the meaning given to that term in Part 3 of this Addendum.

Permitted Purpose: has the meaning given to that term in Part 1 of this Addendum.

Personal Data: means any and all personal data that is processed by us pursuant to or in connection with the Agreement irrespective of our role, including Joint Data, Controller Data and Processor Data.

Personnel: means, in respect of a party or a member of its Group, their directors, officers, employees, consultants, agents, servants and contractors and such persons of their sub-contractors (as applicable to each party).

Privacy Notice: means IFX's privacy notice which is available on the Website and which may be updated from time to time by IFX.

Processing Instructions: has the meaning given to that term in paragraph 1 of Part 4 of this Addendum.

Processor Data: has the meaning given to that term in Part 4 of this Addendum.

Relevant Laws: means all laws, regulations, regulatory requirements, obligations, or rules in the United Kingdom that apply to this Agreement, including any binding codes of conduct or statements of principle incorporated into or contained in such rules from time to time, when applicable, according to any guidance, code of conduct, or other similar document published by any Relevant Regulatory Authority.

Relevant Payment System Operator: means a person who has managerial or operational responsibility for a payment system, as defined in Section 42(3) of the Financial Services Banking Reform Act 2013.

Relevant Regulatory Authority: means a regulatory body that has authority over one or both of the parties with regard to the delivery or receipt of the Services or the fulfilment of the parties' obligations under the Agreement. Examples of such bodies include the UK Financial Conduct Authority, the UK Prudential Regulatory Authority, the Bank of England, the European Commission, HM Treasury, the UK Competition and Markets Authority, any tax authority, a payment systems regulator, and any Supervisory Authority.

Services: means the services received or to be received by the Client or its Group under the Agreement.

Sub-Processor: means a different processor that we have employed to perform processing activities relating to the Processor Data under or in connection with the Agreement.

Supervisory Authority: refers to any entity, whether local, national, or multinational, that is responsible for administering the Data Protection Legislation, including the Information Commissioner's Office, as well as any agency, department, official, parliament, public or statutory person, government or professional body, regulatory or supervisory authority, or board that falls under this definition.

TPP: means a third party provider as defined by the Payment Services Regulations 2017 (SI 2017/752) (PSR), which includes an Account Information Service Provider (AISP), a Payment Initiation Service Provider (PISP), and/or a Confirmation of Payee service provider (CBPII).

Website: means www.ifxpayments.com.

1.2. A person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).

1.3. A reference to a party includes its successors and permitted assigns.

1.4. A reference to legislation or a legislative provision is a reference to it as amended or re-enacted. A reference to legislation or a legislative provision includes all subordinate legislation made under that legislation or legislative provision.

1.5. Any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

1.6. Terms such as "personal data," "personal data breach," "processing," "processor," "controller," "joint controller," and "data subject," which are used but not defined in this Addendum, have the meanings outlined in the Data Protection Legislation.

1.7. Unless the context dictates otherwise, and subject to the definition of "Data Protection Legislation" in clause 1.1 above, any reference to European Union law that is directly applicable or directly effective in the United Kingdom at any time refers to it as it applies in the EEA, including in any retentions, amendments, extensions, or re-enactments that take effect on or after 31 January 2020.

1.8. "*you*" or "*your*" refers to your company or organisation. When "*you*" or "*your*" refers to two or more people, it refers to each individual as well as the group as a whole.

1.9. In this Addendum, references to paragraphs refer to those in that paragraph, and references to Parts refer to those in that Part.

1.10. Phrases beginning with "including," "include," "in particular," or other similar expressions are to be understood as illustrative and not as limiting the meaning of the words that come before them.

1.11. We reserve the right to periodically update this Addendum in order to address changes to the Services, such as any new functionality or features, to address our obligations under the Data Protection Legislation, and/or to address any additional services that we may offer you from time to time. Notice shall be deemed to have been provided on the date of publication of the Addendum on the Website, and the provisions of the most recent version of this Addendum made accessible on the Website will apply.

PART 1

GENERAL TERMS

1. Data Processing

1.1. We will process personal data in connection with providing or receiving the Services, or in anticipation of providing any services, in order to fulfil our obligations under the Agreement, for our legitimate business purposes (such as complying with legal and regulatory requirements, IT security, and administrative purposes), and in accordance with the Privacy Notice (the **Permitted Purpose**).

1.2. We will maintain any necessary registrations and pay any applicable fees to our national Supervisory Authority to cover the processing activities described in the Permitted Purpose.

1.3. We have designated a Data Protection Officer who can be contacted at privacy@ifxpayments.com with any questions or concerns regarding this Addendum or the processing of personal data by us.

2. Data Security

2.1. The Services have been developed with IT security and Data Protection Legislation in mind.

2.2. To ensure the security, integrity, availability, and confidentiality of the Personal Data, and protect against unauthorised or unlawful processing of the Personal Data and accidental loss or destruction of, or damage to, the Personal Data, we have implemented and will maintain appropriate technical and organisational measures. These measures will 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, taking into account the state of technological development and the cost of implementing any measures.

2.3. We have the following measures in place:

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

2.3.2. **Encryption** - Personal Data is encrypted at rest and in transit.

2.3.3. **Monitoring and Testing** - We have in place a process for regularly testing, assessing and evaluating the effectiveness of our security measures.

2.3.4. **Data Backup** - Personal Data is backed up according to an agreed backup schedule.

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

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

3. Training

We will provide our Personnel with adequate training to ensure that they process Personal Data in compliance with the Data Protection Legislation. The training provided will be proportionate to the role, responsibility, and frequency with which the Personnel process Personal Data. We will maintain and review records of the training received by our Personnel. All staff will receive annual training on Data Protection Legislation and the processing of Personal Data, at a minimum.

4. Using Staff and Other Processors

4.1. We may involve Processors or Sub-Processors in processing Personal Data. A complete list of the Processors or Sub-Processors we engage to process personal data on our behalf, together with the location of processing, is available on the Website.

4.2. We will:

4.2.1. establish a written contract with each Processor or Sub-Processor that will limit its processing activities to only what is necessary for its engagement by us in connection with this Agreement and oblige it to comply with terms and conditions that offer substantially the same level of protection for Personal Data as those set out in this Part 1 of this Addendum.

4.2.2. assume responsibility for the acts and omissions of any Processor or Sub-Processor in performing its data processing obligations under this Agreement, as if they were our own.

4.3. We will ensure that all Personnel authorised by us (or any Processor or Sub-Processor) to process Personal Data are bound to maintain the confidentiality of such data (except when disclosure is mandatory in line with Relevant Laws, in which case, where practical and not prohibited by Relevant Laws, we will notify you of the requirement before disclosing such information).

4.4. You consent to our use of the Processors or Sub-Processors set out on the Website.

5. Records and Audits

5.1. In accordance with the Data Protection Legislation, we are obligated to maintain accurate, complete, and up-to-date records of our processing activities (**Records**).

5.2. We will comply with the Data Protection Legislation and provide you access to the Records, except in cases where it would violate Relevant Laws. In such cases, we will inform you to the extent allowed by Relevant Laws. We will also cooperate with audits and inspections conducted by you or an auditor you have authorised in writing, subject to the conditions outlined in paragraph 5.3 of this Part 1 of this Addendum.

5.3. You are required to fulfil the following obligations in relation to information requests, inspections, and audits:

5.3.1. Give us reasonable written notice (not less than ten (10) Business Days) before any information request is made.

5.3.2. Keep confidential all Records and information obtained or generated by you or your auditor in connection with such requests, inspections, and audits, and not disclose them to any third party unless required by a Relevant Regulatory Authority. If such disclosure is necessary, you must give us prior written notice (not less than fourteen (14) days before).

5.3.3. Ensure that such audits or inspections are conducted during our normal business hours, with minimal disruption to our business and the business of our other clients.

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

5.3.5. Comply with any additional obligations related to access by you or an auditor, as specified in the Agreement.

5.4. Please note that nothing in paragraph 5 of this Part 1 of this Addendum gives you the right to access any data of any other client of ours or any information that may

cause us to breach our obligations under Relevant Laws or our confidentiality obligations to a third party.

6. Data Transfers

6.1. We will not transfer your Personal Data to any country or territory outside of the European Economic Area or United Kingdom, including to a Sub-Processor located in such a country or territory, unless:

6.1.1. That country or territory has been deemed adequate by the European Union under Article 45 GDPR, or by other means provided under the Data Protection Legislation.

6.1.2. We have taken measures to ensure that any such transfer complies with the Data Protection Legislation by implementing Appropriate Safeguards. We have also verified that:

6.1.2.1. The level of protection provided to the Personal Data in the destination country or territory is equivalent to that which would be provided to Personal Data in the EEA or UK.

6.1.2.2. Any data importer has provided us with relevant information on the destination country or territory and the applicable laws to support the claim in 6.1.2.1.

6.1.2.3. Any data importer is contractually obliged to inform us of any developments that could affect the level of protection given to your transferred Personal Data in the importer's country.

6.1.3. We are permitted to do so by derogation under Article 49 of the GDPR, or as otherwise specified under the Data Protection Legislation.

6.2. If, for any reason, the transfer of Personal Data under paragraphs 6.1.1, 6.1.2, or 6.1.3 of this Part 1 of this Addendum becomes unlawful, we will promptly apply other Appropriate Safeguards and make sure that the level of protection afforded to your Personal Data in the destination country or territory is equivalent to that which would be provided to Personal Data in the EEA or UK. If we are unable to do so, we will stop such transfer of Personal Data, unless you have expressly authorised it to continue.

7. Data Retention

7.1. We will ensure that we do not keep Personal Data for any longer than is needed to achieve the Permitted Purpose.

7.2. We will adhere to our data retention policy.

8. Reporting

8.1. In accordance with the Data Protection Legislation, we will fulfil our responsibilities to report any personal data breach to the relevant Supervisory Authority and, if necessary, to the affected data subjects.

8.2. If we are made aware of any personal data breach in connection with the Services, we will promptly inform you within 48 hours and provide all necessary information about the breach. We will also cooperate with you and provide reasonable assistance to ensure that the breach is handled in a compliant and timely manner and to help us meet our obligations under the Data Protection Legislation. We will not disclose any information about the breach unless required by law or a Supervisory Authority, in which case we will notify you beforehand.

8.3. We will promptly investigate any personal data breach involving Personal Data and take appropriate measures to prevent, mitigate, and rectify any negative effects of such a breach.

8.4. We will keep you reasonably informed of any developments related to any personal data breach.

9. Your Obligations

9.1. Regardless of whether we act as a joint controller, controller, or processor, you have the following obligations:

9.1.1. You must independently determine 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 must comply with your obligations as a controller or joint controller (as applicable) and provide services to Clients in compliance with the Data Protection Legislation.

9.1.3. You must maintain any valid registrations and pay any fees required by your Supervisory Authority to cover your processing activities, including those contemplated under the Agreement.

9.1.4. You must maintain adequate data processing, privacy, and IT security policies in relation to your processing of personal data and any cybersecurity incidents that meet the requirements of the Data Protection Legislation. You must comply with and ensure that your Personnel comply at all times with such policies.

9.1.5. You must ensure that your Personnel are subject to written confidentiality obligations that cover their processing of Personal Data.

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

9.1.7. If we request it, you must promptly provide reasonable evidence to us that you have provided all necessary information and notices to and obtained all necessary consents from data subjects and otherwise complied with your obligations under the Data Protection Legislation.

9.1.8. We are entitled to assume that any disclosure or transfer of personal data to us by you (directly or indirectly) is done so in a manner that is compliant with the Data Protection Legislation.

9.1.9. You must ensure that any personal data you disclose or otherwise transfer to us is accurate.

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

9.1.11. You must notify us promptly (and in any event within forty-eight (48) hours) if you become aware of a personal data breach by us or otherwise in connection with the Services and provide us with full details of the personal data breach. You must 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 must not release or publish any filing, communication, notice, press release, or report concerning any personal data breach by us or otherwise in connection with the Services unless required to do so under the Data Protection Legislation and/or by a Supervisory Authority. If required to do so, you must notify us in advance of such requirement.

9.1.12. In the event that you receive or become aware of a Data Complaint, you shall promptly notify us within 2 (two) Business Days, to the extent permitted by law. You shall also provide us with reasonable assistance and cooperation as necessary to address such Data Complaint.

9.1.13. You agree to provide us with reasonable assistance and cooperation as needed to fulfil our obligations under the Data Protection Legislation. Such obligations may include those related to security, handling Data Subject Requests, conducting data protection impact assessments, and consulting with a Supervisory Authority.

9.1.14. You shall comply with any additional obligations that may be imposed on you in other parts of this Addendum.

PART 2

CONTROLLER TERMS

If we process personal data as an independent controller under or in connection with the Agreement, including Controller Data, the provisions outlined in Part 2 of this Addendum will apply to the processing of Controller Data, in addition to the General Terms in Part 1 of this Addendum.

1. Processing Controller Data

1.1. We will comply with our obligations as a controller under the Data Protection Legislation in relation to our processing of Controller Data.

1.2. In processing Controller Data, we will:

1.2.1. Only process the data for the Permitted Purpose, in accordance with Schedule 1 of this Addendum, and any updates made from time to time.

1.2.2. Provide all necessary, fair, and transparent information and notices to data subjects, including details on the processing of personal data required for the Permitted Purpose, the legal basis for the processing, recipients of the personal data (including Relevant Payment System Operators and Relevant Regulatory Authorities), and any other information required to be given by a controller under the Data Protection Legislation.

1.2.3. Ensure that data subjects can easily access a point of contact to make a Data Subject Request relating to their Controller Data.

2. Data Subject Requests

2.1 If you receive a Data Subject Request and/or a Data Complaint related to the processing of Controller Data, you must promptly notify us via email at privacy@ifxpayments.com (and in any event within two (2) Business Days of receiving the request/complaint), and unless otherwise required by Relevant Laws or a Supervisory Authority, we will be responsible for and handle the Data Subject Request and/or Data Complaint in compliance with the Data Protection Legislation.

PART 3

JOINT CONTROLLER TERMS

In cases where the parties jointly control or otherwise process personal data in connection with the Agreement (referred to as **Joint Data**), the provisions outlined in Part 3 of this Addendum shall apply to the processing of Joint Data in addition to Part 1 of this Addendum.

1. Processing of Joint Data

1.1. Each party shall comply with its controller obligations as required by Data Protection Legislation with respect to its processing of Joint Data.

1.2. The parties acknowledge and agree that:

1.2.1. they will jointly determine the purpose and means of processing the Joint Data;

1.2.2. they will only process the Joint Data for the Permitted Purpose and in accordance with Schedule 1 of this Addendum, which may be updated periodically;

1.2.3. they will ensure that the Joint Data is collected, processed, and transferred in compliance with applicable Data Protection Legislation;

1.2.4. each party will be responsible for providing any necessary and transparent information and notices to data subjects, detailing the processing of Joint Data for the Permitted Purpose, the legal basis for such processing, the recipients of the Joint Data (including the other party, Relevant Payment System Operators and Relevant Regulatory Authorities), and any other information required to be disclosed by a controller under Data Protection Legislation. The information and notices shall be transparent regarding the arrangement between the parties to comply with Data Protection Legislation;

1.2.5. each party shall cooperate with the other party to provide any information reasonably necessary to enable the other party to produce and publish its information and notices in accordance with paragraph 1.2.4 of Part 3 of this Addendum;

1.2.6. each party shall ensure that any data subject who wishes to make a Data Subject Request has an easily accessible point of contact to do so; and

1.2.7. each party shall reasonably assist the other party in ensuring compliance with its obligations under Data Protection Legislation, in relation to security, personal data breach notifications, data protection impact assessments, and consultations with Supervisory Authorities, insofar as they relate to the processing of Joint Data.

2. Data Subject Requests and Data Complaint Handling

2.1. Upon receiving a Data Subject Request or Data Complaint related to Joint Data processing, a party must promptly inform the other party, no later than two (2) Business Days from receiving the request. The parties will comply with the provisions set out in this clause.

2.2. The party that first receives a Data Subject Request will bear the responsibility of responding to it, and the party that receives a Data Complaint regarding Joint Data processing will bear the responsibility of responding to it, unless the parties agree otherwise.

2.3. The parties will provide reasonable assistance to each other to handle Data Subject Requests and Data Complaints related to Joint Data processing.

2.4. Each party will handle Data Subject Requests and Data Complaints related to Joint Data processing in a professional and timely manner and in compliance with the Data Protection Legislation's requirements, including any time limits.

2.5. Unless responding to a Data Subject Request or Data Complaint will cause a breach of the Data Protection Legislation or is required by a Supervisory Authority, neither party will respond to such requests or complaints without consulting the other party.

3. Personal Data Breaches

3.1. If either party experiences a personal data breach concerning Joint Data processing:

3.1.1. The discovering party will notify the other party without undue delay, and no later than forty-eight (48) hours from becoming aware of the breach. The notification will include a detailed description of the breach, data type, affected persons' identities, and any other relevant information.

3.1.2. The parties will cooperate reasonably to identify the cause of the breach and determine who should notify the Supervisory Authority and/or the data subjects, if necessary. If no agreement is reached, the notifying party will handle the notification.

3.1.3. The party suffering the personal data breach will take immediate action to remedy the situation.

3.2. If you become aware of a personal data breach related to Joint Data, you must notify us via email at privacy@ifxpayments.com.

PART 4

PROCESSOR TERMS

In case we process personal data as a processor for you under or in connection with the Agreement (referred to as **Processor Data**), the processing of Processor Data will be governed by the provisions outlined in this Part 4 of this Addendum, in addition to Part 1 of this Addendum.

1. Instructions and Processing Details

1.1. As a processor, we will process the Processor Data in accordance with the Agreement, Schedule 1, and any documented instructions from you (**Processing Instructions**), unless Relevant Laws require otherwise.

1.2. If Relevant Laws require us to process the Processor Data differently from the Processing Instructions, we will notify you of such requirements before processing the Processor Data, unless prohibited by Relevant Laws on important grounds of public interest.

2. Technical and Organisational Measures

2.1. We will implement and maintain suitable technical and organisational measures to:

2.1.1. Ensure compliance with Data Protection Legislation, including Article 32 GDPR, and protect the rights of data subjects.

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 related to the processing of Processor Data, we will promptly notify you, unless otherwise required under Relevant Laws or by a Supervisory Authority. You will handle the Data Subject Request in compliance with the

Data Protection Legislation, and we will reasonably cooperate and assist you in executing your obligations under the Data Protection Legislation.

3.2. We will provide assistance as reasonably necessary to help you fulfil your obligations under the Data Protection Legislation regarding:

3.2.1. Security of processing.

3.2.2. Data protection impact assessments (as defined in the Data Protection Legislation).

3.2.3. Prior consultation with a Supervisory Authority regarding high-risk processing.

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

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

4. Using Other Processors

We will keep you informed ahead of time before engaging any Processor or Sub-Processor that we have not previously notified you of by directing you to an updated list of Processors or Sub-Processors on the Website. Should you object to the involvement of any new Processor or Sub-Processor, please notify us promptly in writing with reasonable grounds for your objection (**Objection Notice**). Upon receiving your Objection Notice, we will work with you in good faith to address any reasonable objections. If, after ninety (90) days of receiving the Objection Notice, you can demonstrate that we have not complied with paragraph 4.2.1 of Part 1 of this Addendum, you may terminate our Agreement in line with its terms.

5. Information and Audit

We will provide you with necessary information to demonstrate our compliance with the obligations of processors under this Part 4 of this Addendum and the Data Protection Legislation, subject to Relevant Laws. We will also allow audits, including inspections, by you or an auditor mandated by you and agreed by us in writing, as required by Data Protection Legislation or a Supervisory Authority, provided you comply with paragraphs 5.3 and 5.4 of Part 1 of this Addendum.

6. Deletion or Return of Processor Data and Copies

Upon termination of the Agreement and your written request, we will return the Processor Data to you or securely destroy it, unless storage is required by Relevant Laws.

Schedule 1

Data Processing Details

Detail	Description
Subject matter of the Personal Data Processing	The processing of personal data necessary for the Permitted Purpose.
Duration of the Personal Data Processing	During the term of the Agreement and for any period necessary to comply with Relevant Laws.
The nature and purpose of the Personal Data Processing	Processing of personal data necessary to achieve the Permitted Purpose.
The type of Personal Data Processing	The personal information that we receive or collects for the Permitted Purpose includes individuals' identity, contact, financial, transaction, correspondence, usage, security (such as passwords and usernames), technical, publicly available, and marketing and communications data (as outlined in the Privacy Notice).
The categories of Data Subject	The scope of individuals whose personal data is provided by you or at your instruction, associated with you, or processed by us for the Permitted Purpose encompasses partners, directors, shareholders, beneficial owners, company secretaries, trustees, members, employees, clients, payers, payees, and anyone else whose data is processed in connection with the Services or in anticipation of the provision of services.