DATA PROCESSOR AGREEMENT

This data processing agreement forms part of the Money Remittance Agreement from --/--/---- *("Principal Contract")* and is made effective from _____ day of _____, 20___ *between* the undersigned parties: -

(i) **Remittance360 Ltd.,** whose trading address is 85-87 Bayham Street, London, Camden, NW10AG United Kingdom *("Controller")*

And

(ii) **[Processor Name],** whose trading address is **[Processor Trading Address]** *("Processor")*

1.   Terms of Agreement

1.1.   This agreement supplements the Principal Contract and makes legally binding provisions for compliance with the UK GDPR as set forth in this agreement. As per the requirements of UK GDPR, all processing of personal data by a processor on behalf of a controller, shall be governed by a contract. The terms, obligations and rights set forth in this agreement relate directly to the data processing activities and conditions laid out in Schedule 1.

1.2.   The terms used in this agreement have the meanings as set out in the *'definitions'* part of the document.

2.   Definitions

2.1.   In this Agreement, unless the text specifically notes otherwise, the below words shall have the following meanings: -

2.2.   *"Consent"* of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

2.3.   *"Effective Date"* means that date that this agreement comes into force

2.4.   *"Personal Data"* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

2.5.   *UK GDPR"* means the United Kingdom General Data Protection Regulation *(tailored by the Data Protection Act 2018)*

2.6.   *"Principal Contract"* means the main contract between the parties named in this agreement

2.7.   *"Processing"* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

2.8.   *"Recipient"* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with domestic law, shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing

2.9.   *"Third-party"* means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

2.10.   *"Sub Processor"* means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller

2.11.   *"The Commissioner"* means the Information Commissioners Office pursuant to Article 51 of the *GDPR"*

3.   Obligations and Rights of the Processor

3.1. The Processor shall comply with the UK GDPR and must: -

a) only act on the written instructions of the Controller

b) ensure that people processing the data are subject to a duty of confidence

c) ensure that any natural person acting under their authority who has access to personal data, does not process that data except on instructions from the Controller

d) use its best endeavours to safeguard and protect all personal data from unauthorised or unlawful processing, including *(but not limited to)* accidental loss, destruction or damage and will ensure the security of processing through the demonstration and implementation of appropriate technical and organisational measures as specified in Schedule 1 of this agreement

e) ensure that all processing meets the requirements of the UK GDPR and is in accordance with the Data Protection Principles

f) ensure that where a Sub-Processor is used, they: -

     i.   only engage a Sub-Processor with the prior consent of the data controller

     ii.   inform the controller of any intended changes concerning the addition or replacement of Sub-Processors

     iii. they implement a written contract containing the same data protection obligations as set out in this agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the UK GDPR

      iv. understand that where any Sub-Processor is used on their behalf, that any failure on the part of the sub-processor to comply with the UK GDPR or the relevant data processing agreement, the initial processor remains fully liable to the controller for the performance of the Sub-Processor's obligations

g) assist the Controller in providing subject access and allowing data subjects to exercise their rights under the UK GDPR

h) assist the Controller in meeting its data protection obligations in relation to: -

      i. the security of processing

      ii. data protection impact assessments

      iii. the investigation and notification of personal data breaches

i) delete or return all personal data to the Controller as requested at the end of the contract

j) make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the UK GDPR and allow for, and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller

k) tell the Controller immediately if they have done something (*or are asked to do something*) infringing the UK GDPR

l) co-operate with the Commissioner in accordance with the UK GDPR Article 31

m) notify the Controller of any personal data breaches in accordance with the UK GDPR Article 33

n) where applicable, employ a Data Protection Officer if required

3.2. Nothing within this agreement relieves the processor of their own direct responsibilities, obligations and liabilities under the UK GDPR.

3.3. The Processor is responsible for ensuring that each of its employees, agents, subcontractors or vendors are made aware of its obligations regarding the security and protection of the personal data and the terms set out in this agreement.

3.4. The Processor shall maintain induction and training programs that adequately reflect the Data Protection Law requirements and regulations, and ensure that all employees are afforded the time, resources and budget to undertake such training on a regular basis.

3.5. Any transfers of personal data to a third country or an international organisation shall only be carried out on documented instructions from the controller, unless required to do so by domestic law. Where such a legal requirement exists, the Processor shall inform the Controller of that legal requirement before processing.

3.6. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing: -

a) the name and contact details of the Processor(s) and of each Controller on behalf of which the Processor is acting, and, where applicable, the data protection officer

b) the categories of processing carried out on behalf of each Controller

c) transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards

d) a general description of the technical and organisational security measures referred to in Article 32(1)

3.7. The Processor shall maintain records of processing activities in writing, including in electronic form and shall make the record available to the Commissioner on request

3.8. When assessing the appropriate level of security and the subsequent technical and operational measures, the processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

4.   Obligations and Rights of the Controller

4.1. The Controller is responsible for verifying the validity and suitability of the Processor before entering into a business relationship.

4.2. The Controller shall carry out adequate and appropriate onboarding and due diligence checks for all Processors, with a full assessment of the mandatory UK GDPR requirements.

4.3. The Controller shall verify that the Processor has adequate and documented processes for data breaches, data retention and data transfers in place.

4.4. The Controller shall obtain evidence from the Processor as to the: -

a) verification and reliability of the employees used by the Processor

b) certificates, accreditations and policies as referred to in the **due diligence/onboarding questionnaire**

c) technical and operational measures described in ***Schedule 1*** of this agreement

d) procedures in place for allowing data subjects to exercise their rights, including *(but not limited to)*, subject access requests, erasure & rectification procedures and restriction of processing measures

4.5. Where the Controller has authorised the use of any Sub-Processor by the initial Processor, the controller must verify that similar data protection agreements are in place between the initial Processor and Sub-Processor.

4.6. Where the Controller has authorised the use of any Sub-Processor by the initial Processor, the details of the Sub-Processor must be added to ***Schedule 2*** of this agreement.

5.   Penalties & Termination

5.1. By signing this agreement, the Processor confirms that they understand the legal and enforcement actions that they may be subject to should they fail to uphold the agreement terms or

breach the Data Protection Laws. If the processor fails to meet their obligations, they may be subject to: -

   a) investigative and corrective powers of the Commissioner under Article 58 of the UK GDPR

   b) an administrative fine under Article 83 of the UK GDPR

   c) a penalty under Article 84 of the UK GDPR

   d) pay compensation under Article 82 of the UK GDPR

5.2. The Controller or Processor can terminate this agreement by **[insert termination terms and notification periods].**

6.   General Information

6.1. [insert any other clauses or terms specific to this Processor and your business relationship]

IN WITNESS below of the parties or their duly authorized representatives have signed this agreement in accordance with all its clauses and on the day, month and year stated at the top of this agreement.

Signed on behalf of the Processor:

Signed: _____

Print Name: _____

Date: _____

Company Name: _____

Position: _____

Signed on behalf of the Controller:

Signed: _____

Print Name: _____

Date: _____

Company Name: _____

Position: _____

SCHEDULE 1

1. Processing Details

a) The Controller named in this agreement has appointed the Processor with regard to specific processing activity requirements. These requirements relate to of processing personal data of **money remittance clients and the Controller's employees.**

b) The duration of the processing is during the term of the contract and 5 years after its end.

c) The processing activities relate to **money remittance** and are for the purpose of serving the clients by **identifying the remitter and beneficiary and conducting AML checks and performing other control activities required by legislation relating to money remittance.**

d) The requirement for the named Processor to act on behalf of the Controller is with regard to the below type(s) of personal data and categories of data subjects:

   i.   Types of personal data

   - Sensitive personal data

   - General personal data

   - Details of criminal offences

   Personal data may include personal identification details such as name and address, customer relationships, personal finances, family circumstances, residence. Information that a person is included in the sanctions lists.

   ii.   Categories of data subjects

   - Controller employees

   - Money transfer customers

e) The Processor can demonstrate and provide sufficient guarantees as to the implementation of appropriate technical and organizational measures taken to ensure data security and protection: -

   a. **Technical measures:**

   - network equipment (concentrators, commuters, routers etc.) are placed in location protected from 3rd party access;

   - the Processor's employees provide monitoring and administrative support of data security means;

   - database containing personal data and all of its components are physically secured;

   - database users are appropriately identified and authorized for access;

- personal data is encrypted.

    B. **Organizational measures:**

The Processor should provide evidence that he has the following policies and procedures in place:

- Information Security Policy

- Software and hardware information security procedures
- Procedures for employee access to locations where personal data is stored and access to the database
- Contingency plans

f) The obligations and rights of the Controller and Processor are set out in section (2) and (3) of this agreement.

SCHEDULE 2

1. Authorized Sub-Processors

SUB-PROCESSOR NAME	CONTACT DETAILS	PURPOSE OF PROCESSING	TYPE OF DATA PROCESSED	AUTHORISED BY CONTROLLER *(Signature)*

2.

[Include further schedules if applicable/required by the business relationship *(i.e. contract clauses, binding corporate rules etc)*]