SCHEDULE A

DATA PROCESSING AND DATA SECURITY ADDENDUM

This DATA PROCESSING AND DATA SECURITY ADDENDUM ("**Addendum**") constitute an agreement between MoneyGram Payment Systems, Inc. ("**Customer**" or "**MoneyGram**") and you ("**you"** or "**Supplier**") related to your provision of Goods and/or Services to Customer.

WHEREAS, under the terms of the Master Agreement, Supplier may provide Services to Customer which require Supplier to Process Customer Personal Data on Customer's behalf; and,

WHEREAS, the Parties desire to amend and supplement the Master Agreement with the terms of this Addendum which will apply to Supplier's Processing of such Customer Personal Data, including any onward transfers.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions.

1.1 "**Applicable Data Protection Laws**" means all laws and regulations, statutes, rules or administrative requirements in force from time to time as stipulated by any competent authority having jurisdiction over the business of MoneyGram with respect to data protection or privacy, including but not limited to, (i) the Financial Services Modernization Act of 1999, also known as the Gramm–Leach–Bliley Act ("**GLBA**"); (ii) the European Union or EU General Data Protection Regulation 2016/679 ("**GDPR**"); (iii) the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland ("United Kingdom" or "UK") by virtue of section 3 of the EU (Withdrawal) Act 2018 (the "**UK GDPR**") and the UK Data Protection Act 2018 (the "**DPA**") collectively **UK Data Protection Laws**; (iv) to the extent applicable, the California Consumer Protection Act of 2018 ("**CCPA**"); and the data protection or privacy laws, regulations, statutes, rules or administrative requirements in force from time to time of any other state, territory or country applicable to the Processing of Personal Data under the Agreement.

1.2 "**Controller**" means the party which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, or as may be further defined under Applicable Data Protection Laws;

1.3 "**Customer Personal Data**" means any Personal Data which is Processed by Supplier on behalf of Customer.

1.4 "**Data Subject**" means an individual who is the subject of Personal Data.

1.5 **"EEA"** means the European Economic Area.

1.6 "**International Data Transfer Addendum**" means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses approved by the UK Information Commissioner on March 21, 2022.

1.7 "**Personal Data**" means any data that identifies, relates to, is capable of being associated with, or could reasonably be linked to an identified or identifiable natural person or household.

1.8 "**Processing, Processes, Processed or Process**" means any operation or set of operations which are performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as, collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, restricting, erasing, destroying Customer Personal Data.

1.9 "**Processor**" means the Party which Processes Personal Data on behalf of the Controller. A service provider under CCPA is considered a Processor for purposes of this Addendum.

1.10 "**Standard Contractual Clauses**" means the updated standard sets of contractual terms and conditions which have been pre-approved by the European Commission on June 4, 2021, as ensuring appropriate contractual data protection safeguards for Personal Data transfers from the EU/EEA to third countries that do not provide adequate protection to Personal Data.

1.11 "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed.

1.12 "**Subprocessor**" means any third party appointed by or on behalf of the Processor to Process Customer Personal Data.

2. Scope and Structure of this Addendum

This Addendum shall govern the transfer of all Personal Data between the Parties as follows:

2.1. Part I – Global Data Protection Terms sets forth the terms governing the transfer of all Personal Data from Customer to Supplier under the Master Agreement excluding such transfers of Personal Data from the EU/EEA, Switzerland and the UK.

2.2 Part II – Standard Contractual Clauses – Controller to Processor and Processor to Sub-Processor Modules and its Appendix I sets forth the terms governing the transfer of Personal Data from Customer to Supplier under the Master Agreement where Personal Data originating from the EU/EEA or Switzerland is transferred outside of the EEA to a third country that has not been found to provide adequate level of protection to Personal Data by the European Commission.

2.3 Part II. Appendix II – UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses sets forth the terms governing the transfer of Personal Data from Customer to Supplier under the Master Agreement where Personal Data originating from the UK is transferred to a third country that is not covered by the UK adequacy regulations.

2.4. This Addendum is intended to apply to transfer of Personal Data between a Controller and a Processor.

PART I – Global Data Protection Terms

3. Data Protection Terms

3.1 In the context of Supplier's Processing of Customer Personal Data under the Master Agreement, Customer is the Controller of Customer Personal Data and Supplier, the Processor acting on behalf of Customer.

3.2 Supplier shall: (a) comply with all Applicable Data Protection Laws in the Processing of Customer Personal Data, including, but not limited to, security, record keeping, notifying Controller of data breaches and restrictions on international data transfers; (b) assist Customer comply with Applicable Data Protection Laws; and (c) not Process Customer Personal Data other than on Customer's documented instructions. Supplier must promptly notify Customer

if, in its opinion, Customer's instructions would not comply with Applicable Data Protection Laws. Further, Supplier must promptly comply with any Customer request or instruction, requiring Supplier to amend, transfer, or delete Customer Personal Data, or to stop, mitigate, or remedy any unauthorized Processing.

3.3 Supplier agrees and covenants that it shall: (a) keep and maintain all Customer Personal Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure; (b) not Process Customer Personal Data in violation of law; (c) use and disclose Customer Personal Data only for the purposes for which the Customer Personal Data, or access to it, is provided pursuant to the terms and conditions of this Addendum and Master Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Customer Personal Data for Supplier's own purposes or for the benefit of anyone; and (d) not, directly or indirectly, disclose, delete or provide access to, Customer Personal Data to any person other than its authorized employees and representatives, without Customer's prior written consent or as may be required by Applicable Data Protection Laws.

3.4 Supplier will ensure that all its employees and representatives who Process Customer Personal Data: (a) are informed of the Customer Personal Data's confidential nature and use restrictions; (b) have undertaken training on the Applicable Data Protection Laws relating to handling Personal Data and how it applies to their particular duties; (c) are aware both of Supplier's duties and their personal duties and obligations under Applicable Data Protection Laws and this Addendum. Supplier will ensure that employees and representatives who Process Customer Personal Data have agreed in writing, via an employment agreement or other contractual document, to maintain the confidentiality of Customer Personal Data.

3.5 As may be required under Applicable Data Protection Laws, Supplier shall appoint a data protection officer and/or a representative that will ensure compliance with applicable Data Protection Laws.

3.6 Supplier will assist Customer in responding to requests by individuals exercising their rights under Applicable Data Protection Laws. These obligations include Data Subject's rights that may include, but are not limited to, the ability to: (a) access his/her Personal Data held by Customer; (b) request corrections to or erasure of his/her Personal Data held by Customer; and (c) seek to restrict Processing of his/her Personal Data by Customer. Supplier must promptly notify Customer if it receives a request from a Data Subject for access to their Personal Data, or receives any complaint, notice, or communication that directly or indirectly relates to the Personal Data Processing or to any Party's compliance with Applicable Data Protection Laws.

3.7 Unless otherwise agreed to the contrary, Supplier will, at the request of Customer or within ninety (**90**) days of the expiration or termination of the Agreement, destroy or deliver to Customer, and require same from all its Sub-processors, all materials containing Customer Personal Data, together with any and all copies thereof. Notwithstanding the forgoing, Supplier may retain one archived copy as may be required by applicable law, which shall continue to be governed under the terms of this Addendum.

3.8 Supplier will keep detailed, accurate, and up-to-date records of its Processing, including, where applicable: (a) the name and contact information for the Supplier and any representatives, Subprocessors and data protection officers; (b) the categories of Processing activities performed; (c) if Customer Personal Data is transferred to a third country, the details of that

transfer including the safeguards taken; and (d) a description of the technical and organizational security measures implemented in respect of the Processing.

3.9 Supplier will help Customer with data protection impact assessments, privacy impact assessments, or other similar assessments. Supplier will notify Customer in advance of any proposed changes to the way Customer Personal Data is Processed, including proposed use of new technologies, so that Customer can assess whether a data protection impact assessment is needed.

4. Details of Processing. This Section sets out certain information regarding Supplier's Processing of Customer Personal Data under the Master Agreement:

4.1 Subject Matter. The subject matter of the Processing is Customer Personal Data.

4.2 Duration of Processing. The duration of the Processing of the Customer Personal Data is set forth in the Master Agreement and/or the relevant Statement of Work.

4.3 Nature and Purpose. Supplier will Process Customer Personal Data as necessary to perform the Services pursuant to the Master Agreement, as further specified in the Statement of Work, if applicable, and as further instructed by Customer in accordance with this Addendum.

4.4 Type of Customer Personal Data. The Customer Personal Data may include personal details, contact, account and financial information concerning the Data Subjects to the extent necessary to facilitate the Services as contemplated by the Master Agreement and the applicable Statements of Work.

4.5 Categories of Data Subjects. The Data Subjects may include Customer's consumers, employees, suppliers, end users and agents.

5. Subprocessing Of Customer Personal Data. Supplier shall not engage Subprocessor(s) to Process Customer Personal Data without Customer's prior written consent, including Customer's notice of full details of the Processing to be undertaken by the Subprocessor. Supplier will engage Subprocessor(s) only pursuant to a written contract that obligates such Subprocessor(s) to comply with this Addendum. Supplier will remain liable for the actions of its Subprocessers.

6. Restricted Transfers. Supplier shall at all times comply with Applicable Data Protection Laws and the terms of this Addendum with respect to cross border transfer of Customer Personal Data.

7. Data Security.

7.1 Supplier shall implement appropriate technical and organizational measures to protect Customer Personal Data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices, and shall ensure that all such safeguards, including the manner in which Customer Personal Data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable Data Protection Laws, as well as the terms and conditions of this Addendum. These safeguards shall include, but are not limited to: (a) pseudonymisation and encryption of Customer Personal Data; (b) the ability to ensure the on-going confidentiality, integrity, availability and resilience of Processing systems and

services; (c) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of Processing.

7.2 When assessing data security measures, Supplier will consider the risks presented by Processing Customer Personal Data, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data. Security measures will include: (a) limiting access of Customer Personal Data to authorized employees; (b) securing business facilities, data centers, paper files, servers, backup systems and computing equipment; (c) implementing network, application, database and platform security; (d) segregating Customer Personal Data from Supplier's other data; (c) conducting risk assessments, penetration testing and vulnerability scans; (d) implementing appropriate personnel security and integrity procedures and practices, such as background checks consistent with applicable law; and (e) providing appropriate privacy and data security training to employees.

8. Security Breach Procedures.

8.1 Supplier shall put in place an incident report strategy and shall notify Customer of a Security Breach affecting Customer Personal Data without undue delay, but no later than twenty-four (**24**) hours after Supplier becomes aware of it. To the extent known, together with the Security Breach notification, Supplier shall provide to Customer (i) the details of the breach, including, but not limited to, the categories of Personal Data breached and the number of Data Subjects impacted; (ii) the kind of risk the breach is likely to present to the rights and privileges of Data Subjects; and (iii) any security measures, such as encryption and pseudonymisation measures, and any mitigating steps taken by Supplier.

8.2 Immediately following Supplier notification to Customer of a Security Breach, the Parties shall coordinate with each other to investigate the Security Breach. Supplier agrees to cooperate with Customer in Customer's handling of the matter, such as assisting with any investigation, making available relevant records, such as logs, files, and data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise required by Customer. In relation to an identified Security Breach that affects Customer Personal Data, Supplier agrees that it will not notify any third party, including any supervisory authority, government entity or affected data subjects unless specifically directed to do so by Customer unless waiting for such direction would violate applicable law and, in such event, only after notice to Customer and without impairing or limiting Supplier's obligation to cooperate with Customer as set forth in this provision.

8.3 Supplier agrees to maintain and preserve all documents, records, and other data related to a Security Breach and use its best efforts to mitigate damages and prevent a recurrence of any such Security Breach.

9. Customer Audits. Supplier will make available to Customer all information necessary to demonstrate compliance with the obligations in this Addendum and Applicable Data Protection Laws, including, where necessary, permitting Customer and/or its third-party representatives to audit Supplier's compliance with its obligations under this Addendum.

10. Indemnification. In addition to the indemnification obligations set forth in the Master Agreement, Supplier will indemnify and hold harmless Customer for all claims and proceedings and all liability, loss, costs, fine and expenses (including reasonable legal fees) incurred by Customer arising from or in connection with (i) unauthorized Processing of Customer Personal Data by the Supplier, its employees or Subprocessors, (ii) Supplier's failure to comply with its obligations under this Addendum, or (iii) a Security Breach.

11. General.

11.1 The Parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Master Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity unless otherwise required by applicable Data Protection Laws.

11.2 Nothing in this Addendum reduces Supplier's obligations under the Master Agreement in relation to the protection of Personal Data or permits Supplier to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Master Agreement.

11.3 In the event of inconsistencies between the provisions of this Addendum the Master Agreement, or any other agreement between the Parties, the provisions of this Addendum shall prevail unless the Parties specifically agree otherwise in writing.

11.4 This Addendum may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. In the event that any signature is delivered by facsimile transmission or by e-mail delivery of a ".pdf" format data file, such signature shall create a valid and binding obligation of the party executing (with the same force and effect as if such were an original thereof).

PART II

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); and Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Moule Two: Clause 9(a), (c), (d) and (e);

(iv) Module Two: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Module Two: Clause 18(a) and (b); and Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B**.

Clause 7

Intentionally omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in **Annex I.B**.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c)The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d)The data exporter warrants that it has imposed the same data protection obligations on the data

importer as set out in the contract or other legal act under Union or Member State law between the controller and the data export.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d)The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii)the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a)The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b)The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c)The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d)The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e)Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f)The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g)The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least **sixty (60**) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data

importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least **sixty (60**) days in advance thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent– the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority where data exporter is required to appoint a representative pursuant to Article 27(1) of Regulation (EU) 2016/679.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities

– relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([2]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification

shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country

of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Poland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Poland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

IN WITNESS WHEREOF, the Parties hereto have executed this Addendum as of the date first above written.

MONEYGRAM PAYMENT SYSTEMS, INC.	Click or tap here to enter text.
_____	_____
Signature	Signature
_____	_____
By: Name	By: Name
_____	_____
Its: Title	Its: Title
_____	_____
Date:	Date:

APPENDIX I to PART II

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: MoneyGram Payments Systems, Inc.

Address: 1550 Utica Avenue South, St. Louis Park, Minnesota, 55416, USA.

Contact person's name, position and contact details: Global Data Protection Officer, PrivacyGlobalContact@moneygram.com.

Activities relevant to the data transferred under these Clauses: As provided under the Master Agreement and applicable Statement of Work(s) between the Parties.

Signature and date: As provided in the signature page of this Addendum.

Role (controller/processor): Controller.

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred

The categories of data subject transferred are data exporter's (e.g. employees, customers, suppliers, agents etc.)_____

Categories of personal data transferred

The categories of personal data transferred are_____

_____

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

_____

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer shall be on a continuous basis for the duration of the agreement between MoneyGram and Supplier.

Nature of the processing

_____

Purpose(s) of the data transfer and further processing

As provided for in the agreement(s), including Statement of Work between MoneyGram and Supplier.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The personal data will be retained for the duration of the agreement between MoneyGram and Supplier and as further provided under the agreement between the parties.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the processing by (sub-) processors shall be in accordance to the terms of the agreement between MoneyGram and Supplier.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Polish Data Protection Authority: Office for Personal Data Protection, Warsaw, Poland.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Pursuant to the Master Agreement and that certain DATA PROCESSING AND DATA SECURITY ADDENDUM between the data exporter and the data importer, the data importer is obliged to implement appropriate technical and organizational measures to protect the data subjects' personal data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices, and shall ensure that all such safeguards, including the manner in which personal data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws. These measures include, but are not limited to: (a) pseudonymisation and encryption of personal data; (b) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing; (e) processes for user identification and authorization; (f) protection of data during transmission and during storage; (g) ensuring physical security of locations at which personal data are processed; (h) ensuring events logging; (i) ensuing system configuration, including default configuration; (j) measures for internal IT and IT security governance and management; (k) measures for certification/assurance of processes and products; and (l) measures for ensuring data minimization, data quality, limited data retention, accountability, allowing data portability and erasure.

Additionally, when assessing data security measures, the data importer will consider the risks presented by processing personal data, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data. Security measures will include: (a) limiting access of personal data to authorized employees; (b) securing business facilities, data centers, paper files, servers, backup systems and computing equipment; (c) implementing network, application, database and platform security; (d) segregating data exporter's personal data from data importer's other data; (c) conducting risk assessments, penetration testing and vulnerability scans; (d) implementing appropriate personnel security and integrity procedures and practices, such as background checks consistent with applicable law; and (e) providing appropriate privacy and data security training to employees.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

---

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: _____

   Address: _____

   Contact person's name, position and contact details: _____

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): _____

2. …

APPENDIX II to PART II

UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the UK Information Commissioner for Parties making restricted transfers. The Information Commissioner considers that it provides appropriate safeguards for restricted transfers when it is entered into as a legally binding contract.

ANNEX I

Part 1 SECTION 1: PARTIES

1.1. Start date: _____.

1.2. The Parties

Exporter (who sends the Restricted Transfer)

Full legal name: _____.

Trading name (if different): _____.

Main address (if a company registered address): _____.

Official registration number (if any) (company number or similar identifier): _____.

Key Contact: _____.

Signature and date: _____.

Importer (who receives the Restricted Transfer)

Full legal name: _____.

Trading name (if different): _____.

Main address (if a company registered address): _____.

Official registration number (if any) (company number or similar identifier): _____.

Key Contact: _____.

Signature and date: _____.

SECTION 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

2.1. Addendum EU SCCs

The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module: 2.

Module in operation: Module 2.

Clause 7 (Docking Clause): Deleted.

Clause 11 (Option): Included.

Clause 9a (Prior Authorisation or General Authorisation): General Authorisation.

Clause 9a (Time period): 60 days.

Is personal data received from the Importer combined with personal data collected by the Exporter?: _____.

SECTION 3: APPENDIX INFORMATION

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: _____.

Address: _____.

Contact person's name, position, and contact details: _____.

Activities relevant to the data transferred under these Clauses: _____.

Signature and date: _____.

Role (controller/processor): Controller.

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: _____.

Address: _____.

Contact person's name, position, and contact details: _____.

Activities relevant to the data transferred under these Clauses: _____.

Signature and date: _____.

Role (controller/processor): Processor.

Annex 1B: Description of Transfer:

1.1. Categories of data subjects whose personal data is transferred: _____ (e.g., customers, employees)
Categories of personal data transferred: _____ (e.g., consumers' name, contact information, financial information, employees' position, bank details).
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: N/A.
The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): on a continuous basis for the duration of the agreement between MoneyGram and Agent.
Nature of the processing: relationships between MoneyGram and Agent.
Purpose(s) of the data transfer and further processing: _____ (e.g., for the provision of MoneyGram services to consumers consistent with the agreement(s) between MoneyGram and Agent).
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: _____ (e.g., for as long as necessary for the purposes for which the personal data was collected for the duration of the agreement between MoneyGram and Agent and as set forth in the agreement(s) between MoneyGram and Agent).
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: the subject matter, nature, and duration of the processing applicable for the data importer are applicable to (sub-) processors as well.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

The Importer is obliged to implement appropriate technical and organizational measures to protect the data subjects' personal data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices, and shall ensure that all such safeguards, including the manner in which personal data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws.

These measures include, but are not limited to: (a) pseudonymisation and encryption of personal data; (b) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing; (e) processes for user identification and authorization; (f) protection of data during transmission and during storage; (g) ensuring physical security of locations at which personal data are processed; (h) ensuring events logging; (i) ensuing system configuration, including default configuration; (j) measures for internal IT and IT security governance and management; (k) measures for certification/assurance of processes and products; and (l) measures for ensuring data minimization, data quality, limited data retention, accountability, allowing data portability and erasure.

Annex III: List of Sub processors (Modules 2 and 3 only)

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: _____.

   Address: _____.

   Contact person's name, position, and contact details: _____.

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): _____.

SECTION 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

4.1. Ending this Addendum when the Approved Addendum changes

Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: Importer and Exporter.

ANNEX II

SECTION 1 ALTERNATIVE PART 2 MANDATORY CLAUSES:

Mandatory Clauses of the Approved Addendum, being 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 **Error! Reference source not found.** of those Mandatory Clauses.