DATA PROCESSING AGREEMENT

version 2.0 update 10.10.2025

THIS DATA PROCESSING AGREEMENT ("DPA") Paysend entity ("Processor")

is subject to and forms part of the Master Agreement entered into between the applicable Paysend entity ("Processor") and the applicable Customer entity ("Controller") that is a party to that agreement. Paysend and Controller shall be collectively referred to herein as "Parties" and individually as a "Party".

This Data Processing Agreement (DPA) sets out the additional terms, requirements, and conditions on which the Processor will process Personal Data when providing services under the Master Agreement.

AGREED TERMS

TERMS, DEFINITIONS, AND INTERPRETATION

Authorised Persons: the persons or categories of persons that the Controller authorises to give the Processor written personal data processing instructions as identified in **ANNEX A** and from whom the Processor agrees solely to accept such instructions.

Business Purposes: the services to be provided by the Processor to the Controller as described in the Master Agreement and any other purpose specifically identified in **ANNEX A.**

Controller: (i) under the GDPR, the Controller, a legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data, and is responsible for ensuring that such processing complies with the GDPR; (ii) under the CCPA/CPRA, the Business that determines the purposes and means of the collection, use, and disclosure of personal information, and is responsible for compliance with consumer rights and statutory obligations under California law; (iii) under PIPEDA, the Organization that determines the purposes and means of the collection, use, or disclosure of personal information, and remains accountable for the protection of such information under Canadian privacy principles.

Data Subject: (i) under the GDPR, an identified or identifiable natural person to whom the Personal Data relates; (ii) under the CCPA/CPRA, a natural person who is a California resident, including a consumer or household, as defined in Cal. Civ. Code §1798.140(g); and (iii) under PIPEDA, an identifiable individual about whom an organization collects, uses, or discloses personal information in the course of commercial activities.

Data Protection Legislation: means all applicable laws, regulations, and other legally-binding requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data under this DPA, including without limitation, solely to the extent applicable, the General Data Protection Regulation, Regulation (EU) 2016/679 **("EU GDPR"**); the United Kingdom Data Protection Act of 2018 ("**UK GDPR"); t**he Personal Data Protection and Electronic Documents Act, S.C. 2000, c. 5 of Canada along with any successor laws and regulations that have the same general intent and effect (**Canada PIPEDA**), the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (as amended and together with its regulations, the "**US CCPA**"). For the avoidance of doubt, if a Party's activities involving Personal Data are not within scope of a given Data Protection Law, such law is not applicable for purposes of this DPA.

Processor: (i) under the GDPR, a Processor, a legal person that processes personal data on behalf of the Controller and is subject to the obligations and restrictions set forth in Article 28, including acting only on documented instructions; (ii) under the CCPA/CPRA, a Service Processor or Contractor that processes personal information for a Business pursuant to a written contract and agrees not to retain, use, or disclose the information for any purpose other than the specified business purpose, nor to sell or share it; (iii) under PIPEDA, a Service Processor or third party that processes personal information on behalf of an Organization in accordance with instructions and with contractual safeguards that ensure a comparable level of protection as required by Canadian privacy law.

Personal Data Breach and Processing, Commissioner: have the meanings given in the Data Protection Legislation.

Personal Data / Personal Information: (i) under the EU/UK GDPR, any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, or online identifier. (Article 4(1), GDPR); (ii) under the California CCPA/CPRA, information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. (Cal. Civ. Code §1798.140(v)(1)); (iii) under Canada's PIPEDA, information about an identifiable individual. (Section 2(1), PIPEDA).

Records: has the meaning given in Clause 12.

Subcontractor (Sub-processor): means any Processor appointed by or on behalf of Processor to process Personal Data on behalf of the Controller in connection with the Agreement. Sub-Processors may include third parties or/and Paysend's Affiliates.

Term: this Agreement's term as defined in Clause 9.

1. **This Agreement** is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Agreement.

The Annexes (Annex A, Annex B, Annex C) form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

In the case of conflict or ambiguity between:

a. any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

b. the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

c. any of the provisions of this Agreement and the provisions of the Master Agreement conflict, the provisions of this Agreement will prevail.

2. Personal data types and processing purposes

The Controller and the Processor agree and acknowledge that for the purpose of the Data Protection Legislation:

a. The Controller retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required

notices and obtaining any required consents, and for the written processing instructions it gives to the Processor.

b. Annex A describes the subject matter, duration, nature, and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Processor may process the Personal Data to fulfil the Business Purposes.

3. Processor's obligations

a. The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Controller's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Processor must promptly notify the Controller if, in its opinion, the Controller's instructions do not comply with the Data Protection Legislation.

b. The Processor must comply promptly with any Controller written instructions requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

c. The Processor will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Controller or this Agreement specifically authorises the disclosure, or as required by a law, court, or regulator. If a law, court, or regulator requires the Processor to process or disclose the Personal Data to a third-party, the Processor must first inform the Controller of such legal or regulatory requirement and allow the Controller to object or challenge the requirement, unless the law prohibits the giving of such notice.

d. The Processor will reasonably assist the Controller, at no additional cost to the Controller, with meeting the Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the relevant regulator under the Data Protection Legislation.

e. The Processor must notify the Controller promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Processor's performance of the Master Agreement or this Agreement.

f. The Processor certifies that it shall not sell or share the personal data, retain, use, or disclose the data outside the scope of the contract with the Controller, under the California Consumer Privacy Act.

g. The Processor shall act as an independent Controller where it processes personal data in order to comply with applicable laws and regulations, including but not limited to anti-money laundering (AML), counter-terrorism financing (CTF), sanctions screening, and fraud prevention requirements.

4. Processor's employees

The Processor will take reasonable steps to ensure the confidentiality, the reliability, integrity, and trustworthiness of and conduct background checks consistent with applicable domestic law on all of the Processor's employees with access to the Personal Data.

5. Security

a. The Processor must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Annex B.

b. The Processor must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

i. the pseudonymisation and encryption of personal data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

iv. a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

The Processor will without undue delay notify the Controller in writing if it becomes aware of:

a. the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Processor will restore such Personal Data at its own expense as soon as possible.

b. any accidental, unauthorised or unlawful processing of the Personal Data; or

c. any Personal Data Breach.

Where the Processor becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Controller with the following written information:

1. description of the nature of (a), (b), and/or (c), including the categories of in-scope Personal Data and the approximate number of both Data Subjects and the Personal Data records concerned;
2. the likely consequences; and
3. a description of the measures taken or proposed to be taken to address (a), (b), and/or (c), including measures to mitigate its possible adverse effects.

Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Processor will reasonably co-operate with the Controller at no additional cost to the Controller, in the Controller's handling of the matter, including assisting with any investigation.

The Processor agrees that the Controller has the sole right to determine:

a. whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Controller's discretion, including the contents and delivery method of the notice; and

b. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7. Transfers of personal data

7.1. Controller acknowledges and consents that some technical and data centre support will be supplied by Paysend Affiliates located outside of the UK and EU, depending on the scope of Services and as such, Personal Data may be Processed by those Paysend teams or Affiliates, who may be based in any country, except for sanctioned countries.

7.2. If the processing personal data involves a Party (or Parties) established outside the UK, EU, or EEA, and the personal data is transferred to a country without an adequacy decision or equivalent safeguards, the relevant provision Annex C shall comprise the EU Standard Contractual Clauses (SCCs), together with the UK Addendum, where applicable. Where required by law, the Processor will conduct and retain a Transfer Impact Assessment before any restricted data transfer.

The current text of the EU SCCs is available at: *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en*.

The current text of the UK Addendum is available at: *https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/*

7.3. Other than those subcontractors (sub-processors) as set out in Annex A, the Processor may not authorise any other third-party or subcontractor to process the Personal Data. The Processor enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Controller's written request, provides the Controller with copies of the relevant excerpts from such contracts;

Those sub-processors approved as at the commencement of this Agreement are as set out in Annex A**.** The Processor maintains an up-to-date list of approved sub-processors, including their names, locations, processing functions, and the contact information for the person responsible for privacy and data protection compliance, and provides such list to the Controller upon request.

8. Complaints, data subject requests, and third-party rights

The Processor must, at no additional cost to the Controller, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Controller as the Controller may reasonably require, to enable the Controller to comply with:

a. the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

b. information or assessment notices served on the Controller by the relevant regulator under the Data Protection Legislation.

The Processor must notify the Controller immediately by email with an attachment original documents if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights, any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9. Term and termination

This Agreement will remain in full force and effect so long as the Master Agreement remains in effect.

If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements.

10. Data return and destruction

On termination of the Master Agreement for any reason or expiry of its term, the Processor will securely delete or destroy or, if directed in writing by the Controller, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

If any law, regulation, or government or regulatory body requires the Processor to retain any documents, materials or Personal Data that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

The Processor will certify in writing to the Controller that it has deleted or destroyed the Personal Data within 60 days after it completes the deletion or destruction.

11. Records

The Processor will keep detailed, accurate, and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control, and security of the Personal Data, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in 5.1 (**Records**).

The Controller and the Processor must review the information listed in the Annexes to this Agreement at least once a year to confirm its current accuracy and update it when required to reflect current practices.

12. Audit

a. At least annually, the Processor will conduct site audits of its Personal Data Processing practices, as well as conduct an independent audit of the Information Technology and Information Security Controls implemented. The Audit Scope shall cover all Processor facilities and systems used for providing services and obligations defined under this Agreement. The Audit shall be carried out by an independent, third-party certification body or auditing firm, and will be conducted based on an industry-recognized and accepted standard or framework (e.g. ISO 27001:2022, System and Organization Controls 2 (SOC 2) AICPA, PCI DSS, etc.). In addition, the Processor shall, on an annual basis, conduct a penetration testing exercise for systems used for providing services and obligations defined under this agreement. The penetration testing exercise shall be carried out by an independent, third-party, accredited Penetration Testing Processor.

b. On the Controller's written request, the Processor will make a summary of its most recent of relevant audit reports available to the Controller for review. The Processor will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Processor's management.

13. Warranties

The Processor warrants and represents that its employees, subcontractors, and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

The Controller warrants and represents that the Processor's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Controller will comply with the Data Protection Legislation.

14. Liability

14.1. To the extent permitted by law, Paysend accepts no liability for any:

1. inaccurate data (including Personal Data) provided to Customer as part of the Services to the extent that such inaccuracy arises from incorrect data provided by Customer, any data subjects or any of the Processor's sources that are not Sub-Processors as defined in this DPA; or
(ii) representations, guarantees or conditions that the Services and/or the Personal Data are fit for a particular purpose or will meet Customer's requirements.

14.2. Notwithstanding any other provision in this DPA and/or the Agreement, the Paysend's total aggregate Liability under this DPA shall be limited to (100%) of the charges paid and/or payable under the Agreement in last 12 months for any one claim in respect of any liabilities, whether arising from tort (including negligence), breach of contract or otherwise under or in connection with this DPA.

14.3. Paysend shall not be liable to Customer for any Liabilities, whether in contract, tort (including negligence), for breach of statutory duty or otherwise arising under or in connection with this DPA for:

(i) indirect or consequential loss or special damages; or

(ii) for any loss of profit, revenue, savings, contract, goodwill or business (whether direct, indirect or pure economic losses).

14.4. For the purposes of this DPA, "Liability" means all direct losses, damages, charges, expenses, reasonable legal and other professional costs awarded against Customer or Paysend, as applicable.

.15. Notice

Any notice given to a party under or in connection with this Agreement shall be in writing and shall be sent by email at the time of transmission, or, if this time falls outside Business Hours in the place of receipt, when Business Hours resume to the following addresses

i. For the Controller: _____ email of privacy contact

ii. For the Processor: dataprotection@paysend.com

This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This Agreement has been entered into on the date stated at the beginning of it.

16. ANNEX

Annex A Personal Data processing purposes and details

Annex B Security measures

Annex C Restricted Transfers

ANNEX A. Personal Data processing purposes and details

Subject matter of processing: Paysend provides the Paysend Platform and payment Services

Duration of Processing: The Processor shall process Personal Data for the duration of the Master Agreement

Nature of Processing: Transaction Processing (executing payment orders, cross-border payout, transfer, settlement)

Business Purposes: Processing for providing payment services which enable funds to be sent, paid out from, or transferred to or from the Controller Account via the Paysend Platform

Personal Data Categories: To initiate a transaction, the Company (Controller) will send a Payment Instruction to the Processor that includes, without limitation, the following personal data information:

Party	**Required Information**
Beneficiary (Natural Person)	First name, Last name, Beneficiary Account Identifier (for Store of Value transactions) OR Reference number identifying the transaction (if not terminating in cash)
Sender and Recipient (Natural Person)	First name, Last name, Business name, Address, City, Zip code, Country
Payment	Card number, Amount, Currency, Transaction reference/invoice ID
Both Parties are Corporate Entities	Purpose of Transaction

Data Subject Types: Senders (individuals initiating payments or transfers) and Beneficiaries, Recipients (individuals receiving the funds).

Authorised Persons: (Insert details of employees/others authorised to give written instructions)

Approved Sub-Processors:

For a list of Sub-Processors (including Paysend Affiliates acting as Sub-Processors and Third-Party Processors), please ask us and we shall provide you with the same. Paysend is generally authorised to engage Sub-Processors, subject to providing a list, giving the Controller at least 30 days' prior notice of any new Sub-Processor, and allowing the Controller to object on reasonable grounds. Paysend will ensure they are bound by data protection terms at least as protective as those in this DPA.

ANNEX B . Security measures

The Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by Applicable Data Protection Legislation.

These measures shall include, as appropriate:

- Encryption of personal data both in transit and at rest.
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Processor implemented the technical and organisational data security measures to comply with Data Protection Legislation, which were approved by relevant security certificates such as:

- Paysend ISO 27001:2022 Certificate
- Paysend PCI DSS Certificate

ANNEX C. Restricted Transfers

Definitions

Data exporter is the Controller or Processor located in the EEA (or subject to the GDPR) who transfers personal data to a third country (outside the EEA) or to an international organization.

Data importer is the Controller or Processor located outside the EEA that receives personal data from the data exporter.

1.1. C2P Restricted Transfers

In respect of any C2P Restricted Transfer subject to the GDPR, the parties hereby enter into Module 2 of the EEA Standard Contractual Clauses (with Customer as data exporter and Controller and Paysend as data importer and Processor), which is hereby incorporated by reference into this DPA and which shall come into effect upon the commencement of a C2P Restricted Transfer. The parties make the following selections for the purposes of Module 2:

(a) Clause 7 (*Docking clause*) shall apply.

(b) Clause 9 (*Use of sub-processors*) option 2 shall apply, and the "*time period*" shall be 30 days.

(c) Clause 11(a) (*Redress*), the optional language shall not apply.

(d) Clause 13(a) (*Supervision*):

(i) Where the Controller is established in an EU Member State, the following shall apply:

"*The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall be the supervisory authority of the Member State in which Controller is established or (if different) the lead supervisory authority of Controller in respect of a cross-border processing activity.*" OR

(ii) Where Controller is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with article 3(2) and has appointed a representative pursuant to article 27(1) of the GDPR, the following shall apply:

"*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, shall act as a competent supervisory authority.*" OR

(iii) Where Controller is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with article 3(2) without, however, having to appoint a representative, the following shall apply:

"*The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as a competent supervisory authority.*"

(e) Clause 17 (*Governing law*) "*Option 1*" shall apply and the "*Member State*" shall be the Republic of Ireland.

(f) Clause 18 (*Choice of forum and jurisdiction*), the Member State shall be the Republic of Ireland.

(g) Annex 1 – the data exporter is Controller, and the data importer is Paysend (in each case as identified, including in relation to their places of establishment, in this DPA), and the processing operations are deemed to be those described in Annex A to this DPA.

1.2. P2C Restricted Transfers

In respect of any P2C Restricted Transfers subject to the GDPR, the parties hereby enter into Module 4 of the EEA Standard Contractual Clauses (with Paysend as data exporter and Processor and Customer as data importer and Controller), which is hereby incorporated by reference into this DPA, and which shall come into effect upon the commencement of a P2C Restricted Transfer. The parties make the following selections for the purposes of Module 4:

(a) Clause 7 (*Docking clause*) of the EU Standard Contractual Clauses shall apply.

(b) Clause 11(a) (*Redress*) of the EU Standard Contractual Clauses, the optional language shall not apply.

(c) Clause 17 (*Governing law*) of the EU Standard Contractual Clauses shall be the Republic of Ireland.

(d) Clause 18 (*Choice of forum and jurisdiction*) of the EU Standard Contractual Clauses, the Member State shall be the Republic of Ireland; and

(e) Annex I of the EU Standard Contractual Clauses shall be deemed to be pre-populated with the relevant sections of Annex A to this DPA.

1.3 Where Paysend receives a Legal Process requiring disclosure of Controller Personal Data to a Public Body, Paysend shall (unless prohibited from doing so by applicable laws) notify Controller of the same. Without prejudice to the foregoing, where the Legal Process places a legally binding obligation on Paysend to disclose Controller Personal Data or to otherwise respond to the Legal Process, Controller acknowledges that Paysend shall be required to Process Controller Data as a Controller in determining its response to that Legal Process.

1.4 In respect of any Restricted Transfer subject to the UK GDPR, the EEA Standard Contractual Clauses (incorporated by reference pursuant to paragraph 1.1 and/or pursuant to paragraph 1.2) shall be read in accordance with, and deemed amended by, the provisions of Part 2 (*Mandatory Clauses*) of the UK IDTA, and the parties confirm that the information required for the purposes of Part 1 (*Tables*) of the UK IDTA is set out in the Agreement, except that for the purposes of Table 4 of Part 1 the parties select the "*neither Party*" option.

1.5. In respect of any relevant transfer between Paysend and a Sub-Processor (P2P), Paysend shall enter into Module 3 of the EEA Standard Contractual Clauses (including, where necessary, as supplemented by the UK IDTA), where doing so is necessary to ensure that the relevant transfer complies with Data Protection Laws.

1.6 For the avoidance of doubt, if, and to the extent that, the European Commission or the UK Government issues any amendment to, or replacement of, the EEA Standard Contractual Clauses or the UK IDTA pursuant to article 46(5) GDPR or article 46 of the UK GDPR, the parties acknowledge and agree that such clauses will automatically be deemed to replace all Standard Contractual Clauses then in force between Controller and Paysend and the parties shall take such additional steps as necessary to give ensure that such replacement terms are implemented across all transfers.

1.7 If, at any time, a supervisory authority or a court with competent jurisdiction over a party mandates that transfers from Controllers in the EEA or the UK to Processors established outside the EEA or the

UK must be subject to specific additional safeguards (including but not limited to specific technical and organisational measures), the parties shall work together in good faith to implement such safeguards and ensure that any transfer of Controller Personal Data is conducted with the benefit of such additional safeguards.

2. UK Personal Data Transfers

2.1. In respect of any transfers of Personal Data under this DPA from the United Kingdom to the extent such transfers are subject to the UK GDPR, for transfers made by the data exporter to the data importer, to the extent that the UK GDPR applies to the data exporter's processing when making that transfer, and to provide appropriate safeguards for the transfers in accordance with Article 46 of the UK GDPR, the Standard Contractual Clause (**Clauses**) are amended as follows:

(a) Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where the UK GDPR applies to the data exporter's processing when making that transfer."

(b) References to "*Regulation (EU) 2016/679*" or "*that Regulation*" or "*GDPR*" are replaced by: "*UK GDPR*" and references to specific Article(s) of "*Regulation (EU) 2016/679*" or "*GDPR*" are replaced with the equivalent Article or Section of the UK GDPR.

(c) References to Regulation (EU) 2018/1725 are removed.

(d) References to the "*European Union*", "*Union*", "*EU*", "*EEA*", "*EU Member State*", "*Member State of the EU*", "*Member State of the EEA*", and "*member state*" are all replaced with the "*UK*".

(e) Clause 13(a) and Part C of Annex II are not used; the "*competent supervisory authority*" is the Information Commissioner's Office ("ICO").

(f) Clause 17 is replaced to state "*These Clauses are governed by the laws of England and Wales".*

(g) Clause 18 is replaced to state:

"*Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts*."

(h) The footnotes to the Clauses do not apply.