

# DATA PROCESSING AGREEMENT

*version 1.0 update 10.10.2025*

**THIS DATA PROCESSING AGREEMENT (“DPA”) Paysend entity (“Controller”)**

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

For the avoidance of doubt, the Parties hereby acknowledge and agree that, in the context of other agreements between them, the respective roles of Controller and Processor may be reversed. The Parties expressly agree that for the purposes of this Agreement, the roles of the Parties shall be as provided herein.

This Data Processing Agreement (DPA) outlines the additional terms, requirements, and conditions under which the Processor will process Personal Data in providing services under the Master Service 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 Service Agreement and any other purpose specifically identified in **ANNEX A**.

**Controller:** (i) under the UK GDPR/EU 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;

**Data Subject:** an identified or identifiable natural person to whom the Personal Data relates;

**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**”); the Protection of Privacy Law, 5741-1981 (PPL) and any other regulation or guidance issued by an applicable supervisory authority relating to the protection of personal data;

**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 outlined in Article 28, including acting only on documented instructions;

**Personal Data Breach:** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed;

**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 PPL, information' means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

**Records:** has the meaning given in Clause 12.

**Restricted Transfer:** means a transfer of Personal Data from the United Kingdom to another country outside the United Kingdom or European Economic Area, subject to restrictions or requirements under the UK GDPR and associated regulations.

**Sub-processor:** means any third party, appointed by or on behalf of the Processor, which will process Personal Data as part of fulfilling the Processor's obligations under this Agreement.

**Supervisory Authority:** means the relevant regulatory authority with responsibility for privacy and data protection in the United Kingdom (the Information Commissioner's Office)

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

The Annexes (Annex A, Annex B) 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 Service Agreement conflict, the provisions of this Agreement will prevail.

## **2. Personal data types and processing purposes**

2.1. 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**

3.1. 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.

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

3.3. 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.

3.4. 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. Where such assistance requires material additional resources beyond the Processor's standard operations, the Parties shall agree in advance on any reasonable costs to be borne by the Controller.

3.5. 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 Service Agreement or this Agreement.

3.6. 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**

4.1. The Processor will take reasonable steps to ensure the confidentiality, 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**

5.1. 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.

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

- a. the pseudonymisation and encryption of personal data;
- b. the ability to ensure the ongoing 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; and
- d. a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

#### **6. Personal data breach**

6.1. The Processor will, without undue delay, within 48 hours, notify the Controller in writing if it becomes aware of and to the extent permitted by applicable law:

- a. the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Processor will make commercially reasonable efforts to promptly attempt to restore such Personal Data;
- b. any accidental, unauthorised or unlawful processing of the Personal Data; or
- c. any Personal Data Breach.

6.2. Where the Processor becomes aware of (a), (b) and/or (c) above, it will, without undue delay within 48 hours, also provide the Controller with the following written information, to the extent such information is available:

- a. 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;
- b. the likely consequences; and
- c. 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.

6.3. 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. Where such assistance requires material additional resources beyond the Processor's standard operations, the Parties shall agree in advance on any reasonable costs to be borne by the Controller.

6.4. The Processor agrees that, subject to applicable law, 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. The Processor shall not transfer any Personal Data outside the United Kingdom without the prior written consent of the Controller, except where such transfer is permitted by Applicable Data Protection Law.

7.2. Where Personal Data is transferred internationally, the parties shall ensure that adequate safeguards are in place, as required by the UK GDPR, or other applicable Data Protection Legislation. This may include reliance on an adequacy decision, Standard Contractual Clauses, or other relevant mechanisms.

7.3. The Processor shall immediately inform the Controller if, in its opinion, further instructions regarding international transfers infringe Data Protection Legislation.

7.4. 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. Those sub-processors approved as at the commencement of this Agreement are as set out in Annex A.

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

8.1. 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.

8.2. The Processor must notify the Controller as soon as reasonably practicable 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**

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

9.2. If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Service 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**

10.1. On termination of the Master Service 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.

10.2. 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 to the extent permitted under such legal 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.

10.3. 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, at Controller's written request.

## **11. Records**

11.1. The Processor will keep detailed, accurate, and up-to-date written records in order to demonstrate Processor's compliance with the Data Protection Legislation and/or this DPA (**Records**).

11.2. 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**

12.1. At least annually, upon no less than thirty (30) days' prior written notice and during normal business hours, the Processor shall allow the Controller or an independent auditor third-party Certification Body or Auditing Firm, to conduct audits and inspections related to the Processor's compliance with its obligations under this Agreement and applicable data protection laws, provided that any such auditors be subject to written and/or statutory confidentiality obligations.

12.2. 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.

12.3. The Processor shall provide the Controller or its auditor with all information reasonably necessary to demonstrate compliance with this DPA, including access to the Processor's facilities, systems, records, processes, and personnel involved in the processing of Personal Data, subject to the Processor's applicable policies.

12.4. On the Controller's reasonable written request and no more than once per calendar year, the Processor will make a summary of its most recent relevant audit reports available to the Controller for review. The Processor will address any material exceptions noted in the audit reports with the development and implementation of a corrective action plan.

12.5. Any audit or inspection shall be conducted in a manner that minimizes disruption to the Processor's business operations and respects the Processor's confidentiality obligations and those of its other clients. The Controller and its auditor shall keep all audit findings and information strictly confidential.

## **13. Warranties**

13.1. 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;

13.2. 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

- For the Controller: [dataprotection@paysend.com](mailto:dataprotection@paysend.com)
- For the Processor: \_\_\_\_\_

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 will enter into force on the date when the Master Service Agreement starts.

## 16. Governing law and Jurisdiction

The parties hereby expressly agree that the competent courts detailed in the Master Service Agreement shall be the exclusive jurisdiction regarding any disputes hereunder and this Agreement shall be governed by the laws stipulated in the Master Service Agreement. Notwithstanding the foregoing, the parties further agree that: (i) to the extent that the Standard Contractual Clauses apply and/or EU Member State law is required in connection with this Agreement, the laws of Ireland shall govern and the competent courts in Ireland shall have exclusive jurisdiction regarding all disputes hereunder; (ii) the competent courts in California shall have exclusive jurisdiction and the laws of California shall govern all disputes hereunder relating solely to the CCPA;

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:** Processor provides the Service Platform and payment Services

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

**Nature of Processing:** Transaction Processing and Global Payment Service

**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 Processor's Platform

**Personal Data Categories:** To initiate a transaction, the 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 Beneficiary, Recipients (individuals receiving the funds).

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

**Approved Sub-Processors:**

The Processor 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 within 7 days of such notice. If no objection is received within this period, the engagement shall be deemed approved. Processor 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.

## 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, 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, 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.