SwiftConnect

Schedule D: Data Protection Addendum

1. **Safeguarding Subscriber Data**. SwiftConnect shall use commercially reasonable efforts to safeguard the security of Subscriber Data resident on the Products or otherwise in the possession of SwiftConnect, and shall employ for this purpose information security controls consistent with accepted practice in the industry, Applicable Law, and Appendix 1 (Technical and Organizational Measures Designed to Ensure the Security of Data).

2. **Privacy; SwiftConnect Role as Service Provider**. SwiftConnect shall act solely as a service provider to the Subscriber under this Agreement, and SwiftConnect shall use Subscriber Data solely for purposes of performing the Services for, and providing the SwiftConnect Platform to, the Subscriber. The Subscriber's privacy policy shall govern privacy practices as to Personal Information of Eligible Users and Credentialed Users. To the extent required by Applicable Law, the Subscriber is responsible for ensuring that any and all necessary notices and consents with respect to the Subscriber's processing (or SwiftConnect's processing on behalf of the Subscriber) of Personal Information are obtained.

3. **Compliance with Applicable Law.** The Subscriber and SwiftConnect shall ensure that its processing activities that occur by or in connection with the Agreement comply with Applicable Law. The Subscriber represents and warrants that it has complied and will continue to comply with Applicable Law in respect of its processing of Personal Information and the processing instructions it issues to SwiftConnect. Each Party shall notify the other Party if it can no longer meet its obligations under Applicable Law as it relates to processing of Personal Information; provided, however, that neither Party shall be required to waive any legal privileges or breach any confidentiality obligations in order to comply with this Section 3 (Compliance with Applicable Law). The Subscriber shall have sole responsibility for the accuracy, quality, and legality of Personal Information and the means by which the Subscriber acquired the Personal Information.

4. **Processing.** SwiftConnect shall process Personal Information for the duration of the Agreement (subject to Section 13 (Retention, Deletion, or Return)) in accordance with the Subscriber's documented instructions, as necessary to comply with Applicable Law, and as necessary to provide the Services, which may include (i) verifying or maintaining the quality or safety of the SwiftConnect Platform or other SwiftConnect products; (ii) undertaking activities to improve, upgrade, or enhance the SwiftConnect Platform or other SwiftConnect products, or internal research for technological development and demonstration; or (iii) detecting data security incidents or to protect against malicious, fraudulent, or illegal activity.

5. **Statistical Data**. Notwithstanding anything to the contrary herein, SwiftConnect shall be entitled to collect, compile, analyze, and otherwise use and exploit (i) statistical data related to the use of the SwiftConnect Platform and System Documentation; (ii) metadata that SwiftConnect collects in connection with the Subscriber's use of the SwiftConnect Platform or System Documentation, including, without limitation, usage data collected for the purpose of billing, maintaining the security of the SwiftConnect Platform or System Documentation, or optimizing the SwiftConnect Platform or System Documentation; and (iii) other data that qualifies as De-Identified Data (collectively, the "**Statistical Data**"). The term "**De-Identified Data**" means information from which personal information has been deleted, masked, or suppressed, and information that has been anonymized, all in manner such that the information (i) does not identify a particular natural person; (ii) does not identify, by network Internet Protocol address or other identifier a particular device or computer associated with or used by a person; and (iii) is not reasonably linkable to a particular natural person due to technical, legal, or other controls. No compensation shall be paid by SwiftConnect with respect to its use of the Statistical Data. This Section 5 (Statistical Data) shall survive termination or expiration of the Agreement. SwiftConnect will not attempt to re-identify the data and will obligate any recipients of the data to do the same.

6. **Consumer Requests**. SwiftConnect will provide reasonable assistance to enable the Subscriber to respond to consumer requests under Applicable Law if the Subscriber is unable to do so itself. If SwiftConnect receives consumer requests related to Personal Information (including requests to delete or request to know, or similar, under Applicable Law), SwiftConnect's sole obligation will be to forward such requests to the Subscriber and the Subscriber shall be responsible for responding to and handling such consumer requests.

7. **International Transfers**.

   7.1. **EEA Data Transfers.** To the extent that SwiftConnect is a recipient of Personal Information protected by the General Data Protection Regulation in a country outside of the European Economic Area and its member states (EEA) that is not recognized as providing an adequate level of protection for Personal Information, the Parties agree to abide by and process Personal Information in compliance with the Standard Contractual Clauses (Appendix 2).

   7.2. **UK Data Transfers.** With respect to transfers of Personal Information from the United Kingdom, the Parties shall abide by the Standard Contractual Clauses as supplemented by Appendix 3 (UK Addendum).

   7.3. **Alternate Transfer Mechanism.** To the extent that a court of competent jurisdiction or data protection authority orders that the measures described in this Section 7 (International Transfers) cannot be relied on to transfer Personal Information (within the meaning of Applicable Law), SwiftConnect may implement any additional measures or safeguards that may be reasonably required to lawfully support the transfer of the Personal Information.

8. **Sub-processors.** The Subscriber hereby grants general written authorization to SwiftConnect to appoint Sub-processors to perform specific processing activities on its behalf. The Subscriber approves those sub-processors SwiftConnect has engaged as of the date of the Agreement. Before engaging a new sub-processor, SwiftConnect shall notify the Subscriber (which notice may be by electronic mail and/or posting notice on a portal to which the Subscriber has access). If within five (5) calendar days of receipt of that notice, the Subscriber notifies SwiftConnect in writing of any objection (on reasonable grounds related to data protection), SwiftConnect will use commercially reasonable efforts to resolve the objection. Absence of any objection from the Subscriber shall be deemed consent to the sub-processor.

9. **Security Incident.** Upon becoming aware of a Security Incident, SwiftConnect shall: (i) notify the Subscriber without undue delay, (ii) provide timely information relating to the Security Incident as it becomes known; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. The term "**Security Incident**" means the unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Subscriber Data containing Personal Information on systems managed or otherwise controlled by SwiftConnect. SwiftConnect's notification of or response to a Security Incident under this Section 9 (Security Incident) shall not be construed as an acknowledgment by SwiftConnect of any fault or liability with respect to the Security Incident.

10. **Assistance.** Solely to the extent required by Applicable Law, SwiftConnect will provide reasonable assistance to the Subscriber, at Subscriber's expense, to conduct any data protection impact assessments or prior consultations with data protection authorities.

11. **Audit.** Upon Subscriber's written request at reasonable intervals no more than once per calendar year, SwiftConnect shall provide a summary of its then most recent third-party SOC 2 audit to Subscriber; provided, however, that (i) all such summaries and information therein shall be considered SwiftConnect Confidential Information, and (ii) SwiftConnect shall be entitled to redact (or withhold) any information that (a) does not relate to Subscriber or Subscriber Data, or (b) would compromise or threaten to compromise the security of SwiftConnect's systems or products or the SwiftConnect Platform.

12. **Government Requests.** If SwiftConnect receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to or information about the Subscriber (including Personal Information) and the Subscriber's primary contact information indicates the Subscriber is located in the EEA or UK, SwiftConnect shall: (i) review the legality of the request; (ii) inform the government agency that SwiftConnect is a processor of the Personal Information; (iii) attempt to redirect the agency to request the Personal Information directly from Subscriber; (iv) notify Subscriber of the request to allow Subscriber to seek a protective order or other appropriate remedy; and (v) provide the minimum amount of information permissible when responding to the agency or authority based on a reasonable interpretation of the request. SwiftConnect shall not be required to comply with this Section 12 (Government Requests) it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or SwiftConnect, but where SwiftConnect is legally prohibited from notifying Subscriber of requests it shall use its best efforts to obtain a waiver of the prohibition.

13. **Return, Deletion, and Return.** Upon termination or expiration of the Agreement, SwiftConnect will delete all Personal Information in its possession in accordance with the Agreement; provided, however, that this obligation will not apply to the extent SwiftConnect is required by Applicable Law to retain some or all of the Personal Information or where SwiftConnect has archived Personal Information on back-up systems.

Appendix 1 to Schedule D: Technical and Organizational Measures Designed to Ensure the Security of Data

1. **Encryption**. SwiftConnect implements measures of pseudonymisation and encryption designed to protect of Personal Information, which may include:
   - 1.1. Adhering to encryption protocols designed to provide effective protection against active and passive attacks;
   - 1.2. Utilizing cloud-based solutions that encrypt data at rest and require that all laptops and desktop disks be encrypted;
   - 1.3. Utilizing transport layer security (TLS), a widely adopted security protocol which includes encryption and authentication of the data as well as a verification of integrity of data in transit;
   - 1.4. Utilizing a third-party cloud platform service which encrypts data at rest with industry standard encryption methods such as Advanced Encryption Standard (AES) AES-256 encryption; and
   - 1.5. Utilizing a third-party payment processing vendor which secures data at rest with industry standard encryption methods such as Advanced Encryption Standard (AES) AES-256 encryption.

2. **System Resilience**. SwiftConnect implements measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services, which may include utilizing an end-to-end compliance audit management software platform to regularly monitor, advance, and promote ongoing compliance with confidentiality, availability and resiliency standards.

3. **Data Restoration**. SwiftConnect implements measures for ensuring the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident, which may include:
   - 3.1. Utilizing a DDoS protection service which provides dynamic detection and automatic inline mitigations that aim to minimize application downtime and latency. It provides comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks;
   - 3.2. Implementing a synchronous mirroring approach in order to prevent data loss and support the ability to restore availability and access to Personal Information in a timely manner in the event of an incident; and
   - 3.3. Adhering to a Business Continuity Plan (BCP) that is designed to manage SwiftConnect's response and communications to key stakeholders by employing the BCP communication protocol. The BCP also includes a full business impact analysis that is designed to detail the potential hazards and challenges to resuming operations.

4. **Testing Controls.** SwiftConnect implements processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing, which may include:

4.1. Performing annual disaster recovery testing by members from management and technical teams to test disaster recovery plans for scenarios such as a cyber-attack or significant infrastructure outage; and

4.2. Conducting third-party cyber vulnerability assessments and penetration testing on a regular basis.

5. **User Identification and Authorization**. SwiftConnect implements measures for user identification and authorization, which may include:

5.1. Utilizing third-party software to automate user provisioning, enable multi-factor identification and facilitate lifecycle management of user access for employees as well as other platform users; and

5.2. Utilizing role-based employee access requirements that require employees to utilize strong passwords (enforced by password requirements) and multi-factor identification (MFA).

6. **Physical Security**. SwiftConnect implements measures for ensuring physical security of locations at which Personal Information are processed, which may include designing and later implementing a security plan for potential future physical locations that may include physical access controls such as professional security staff, video surveillance, visitor management systems, and a process for revoking access when no longer required by the user.

7. **Event Logs**. SwiftConnect implements measures for ensuring logging of Transactions, which may include implementing multiple third-party monitoring systems for audit and log monitoring which are specifically intended to support cloud-based services.

8. **IT Security Governance and Management**. SwiftConnect implements measures for internal IT and IT security governance and management, which may include:

8.1. Requiring all employees to complete security awareness training upon hiring and at least annually thereafter. The training may include topics such as security threats; viruses and other threats; social engineering; security compromises; best practices; passwords; anti-virus and anti-spyware software; firewalls; safety precautions; incident identification; incident response; process in event of incident;

8.2. Conducting regular security risk assessments by the Oversight Committee that is led by SwiftConnect's Chief Information Security Officer (CISO). Risks are documented, assigned likelihood and impact ratings, then assigned a risk priority. Mitigation strategies are developed, and remediation steps and timeline are assigned. The timeline is structured based on the threat severity and technically swiftest schedule permissible. All is documented in the Risk Assessment Matrix, which is reviewed as needed at the monthly Oversight Committee meetings; and

8.3. Maintaining an Oversight Committee comprising senior leadership to determine and assess risks, developing mitigation strategies, and designating remedial measures and timelines as required.

9. **Certification and Assurance**. SwiftConnect implements measures for certification/assurance of processes and products, which may include:

9.1. Requiring all engineers to complete a secure coding course; and

9.2. Utilizing application management platforms to manage and update asset and infrastructure configuration and to track source file changes.

10. **Data Retention**. SwiftConnect implements measures for ensuring limited data retention, data quality, data erasure, and data minimization, which may include adhering to a data retention and disposal process designed to meet customer, legal and regulatory data retention requirements.

11. **Accountability**. SwiftConnect implements measures for ensuring accountability, which may include requiring all employees to complete security awareness training upon hiring and at least annually thereafter. SwiftConnect further ensures that any person authorized to process Personal Information has committed themselves to confidentiality, and that such person will only have access to Personal Information to the extent necessary to perform their job functions.

12. **Subprocessors**. SwiftConnect uses commercially reasonable measures to ensure that its sub-processors and affiliates implement commercially reasonable technical and organizational safeguards commensurate with the size of the organization and scope of information processed by such organization.

Appendix 2 to Schedule D: Standard Contractual Clauses (GDPR)

These Standard Contractual Clauses are incorporated into the Agreement for all purposes to reflect the Parties' agreement related to the processing of the personal data of data subjects. The "data exporter" and "data importer" are specified in Annex I.

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) for the transfer of personal 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) Clause 8.1(b), 8.9(a), (c), (d) and (e); (iii) Clause 9(a), (c), (d) and (e); (iv) Clause 12(a), (d) and (f); (v) Clause 13; (vi) Clause 15.1(c), (d) and (e); (vii) Clause 16(e); and (viii) Clause 18(a) and (b).

(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

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

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 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, upon written request, 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.

Clause 9

Use of sub-processors

(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 30 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. Data exporter may object in writing to data importer's intended changes within five (5) calendar days of receiving notice in accordance with this Clause 9(a).

(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.

Clause 10

Data subject rights

(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.

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) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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;

(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 Ireland.

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 Ireland.

(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.

Annex I to Appendix 2

A. List of Parties

Category	Data Exporter	Data Importer
Business name:	Refer to the Software as a Service Subscription Agreement	SwiftConnect Inc.
Business address:	Refer to the Software as a Service Subscription Agreement	24 Camp Ave. #4890 Stamford, CT 06907
Contact person's name, position and contact details:	Refer to the Software as a Service Subscription Agreement	Privacy Team, privacyteam@swiftconnect.com
Activities relevant to the data		

transferred under these Clauses:	The data importer provides an access and inventory management platform and related services. The data importer will provide the data exporter with certain services agreed in the Agreement.

B. Description of Transfer

This section includes certain details of the processing of the Subscriber's personal data as required by Article 28(3) GDPR or equivalent requirements:

Subject matter and duration of the processing of Subscriber personal data

The subject matter of the processing of the personal data is the provision of the Products and Services to the Subscriber. The personal data will be processed for the duration of the Agreement, subject to section 8.5 of this Appendix.

The nature and purpose of the processing of Subscriber personal data

SwiftConnect shall host, maintain and otherwise process personal data only in connection with the provision of Products and Services pursuant to the terms of the Agreement and this Appendix.

The types of Subscriber personal data to be processed

Personal data input by (or at the direction of) the Subscriber or by data subjects into SwiftConnect's system or that SwiftConnect otherwise processes on the Subscriber's behalf in connection with providing the Products and Services pursuant to the terms of the Agreement and this Appendix, including name, contact information (including, but not limited to: phone, email address) and visitor information (including timestamp of visit).

For certain Products and Services (SwiftConnect Protect), personal data processed by SwiftConnect includes health related information, such as information on symptoms and possible exposure to COVID-19 or a similar/related public health emergency through contact with others, travel and other criteria determined by the Subscriber, collected from data subjects through wellness checks.

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

The data is transferred on a regular and continuous basis.

Nature of the processing

Data is transferred electronically.

The categories of data subject to whom the personal data relate

The Subscriber's employees and visitors.

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

Personal data will be deleted in accordance with provisions of the Agreement, national law requirements, taking into account data storage obligations under applicable labor, tax and other regulatory laws.

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

Name of the Sub-processor	Purpose of the Processing/service provided
Amazon Web Services, Inc	Cloud service provider that provides hosting, storage, and other related services
Detrios, LLC	SwiftConnect subsidiary that provides customer support throughout the customer lifecycle (*e.g.*, onboarding/implementation, ongoing support/debugging)
Google LLC	Cloud service provider that provides hosting, storage email, and other related services
Ipseity Technologies Inc.	SwiftConnect affiliate that provides research and development services
Okta, Inc.	Cloud service provider that provides authentication and identity services
SwiftConnect Canada, Inc.	SwiftConnect subsidiary that provides customer support throughout the customer lifecycle (*e.g.*, onboarding/implementation, ongoing support/debugging)
SwiftConnect UK Ltd.	SwiftConnect subsidiary that provides customer support throughout the customer lifecycle (e.g., onboarding/implementation, ongoing support/debugging)
Zendesk, Inc.	Cloud service provider that provides customer support related services

C. Competent Supervisory Authority

Ireland

Annex II to Appendix 2: Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

SwiftConnect uses the technical and organisational measures set out in Appendix 1 (Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of Data), which is incorporated herein by reference, 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.

Appendix 3 to Schedule D: UK Addendum

Part 1: Tables

Table 1: Parties

The Parties, Details, and Key Contacts: See Annex I to the Standard Contractual Clauses.

Signature and Date: This UK Addendum is deemed to be executed on the date the transfer commenced or the date that the Agreement was executed, whichever is earlier.

Table 2: Selected EU SCCs, Modules and Selected Clauses

Addendum EU SCCs: The version of the Approved EU SCCS, which this UK Addendum is appended to, detailed below, including the Appendix Information.

Date: June 4, 2021

Reference: European Commission decision 2021/914

Module	Module in operation	Clause 7 (Docking Clause)	Clause 9a (Prior Authorization or General Authorization)	Clause 9a (Time period)	Clause 11
2	Controller to processor	Included	General Authorization	30 days	Not included

Table 3: Appendix Information

See, Annex 1 to the Standard Contractual Clauses.

Table 4: Ending this UK Addendum when the Approved Addendum Changes

Which parties may end this UK Addendum as set out in Section 19: Exporter

Part 2: Mandatory Clauses

Entering into this UK Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:
   a. **UK Addendum:** This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
   b. **Addendum EU SCCs:** The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
   c. **Appendix Information:** As set out in Table 3.
   d. **Appropriate Safeguards:** The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
   e. **Approved Addendum:** The template UK Addendum 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 18.
   f. **Approved EU SCCs:** The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
   g. **ICO:** The Information Commissioner.
   h. **Restricted Transfer:** A transfer which is covered by Chapter V of the UK GDPR.
   i. **UK:** The United Kingdom of Great Britain and Northern Ireland.
   j. **UK Data Protection Laws:** All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
   k. **UK GDPR:** As defined in section 3 of the Data Protection Act 2018.

4. This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.
7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this UK Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This UK Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. Together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. This Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this UK Addendum, incorporating the Addendum EU SCCs;
    b. In Clause 2, delete the words: "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";
    c. 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 UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
    d. N/A;
    e. Clause 8.8(i) is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
    f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
    g. References to Regulation (EU) 2018/1725 are removed;
    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
    i. N/A;
    j. Clause 13(a) and Part C of Annex I are not used;
    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
    l. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";
    m. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";
    n. Clause 18 is replaced with: "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."; and
    o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendment to this UK Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:
    a. Makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. Reflects changes to UK Data Protection Laws

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
    a. Its direct costs of performing its obligations under the Addendum; and/or
    b. Its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
20. The Parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.