Citcon Data Processing Addendum

This Data Processing Addendum (“DPA”) is incorporated into, and is subject to the terms and conditions of the Agreement between the CITCON USA LLC. (“Citcon”) and a customer entity, such as a party to an Agreement as a Merchant (“Customer”).

1. Interpretation

In this DPA the following expressions shall, unless the context otherwise requires, have the following meanings:

“Agreement” means any agreement between Citcon LLC. and a customer for Services. Such an Agreement may have various titles, such as “Terms of Use” or “Master Services Agreement”.

“Article 28” means article 28 of GDPR and the UK GDPR as applicable to the processing of Customer Personal Data.

“Customer” or “you” means the customer that is identified on, and/or is a party to, the Agreement.

“Customer Data” means all data (including but not limited to Customer Personal Data) that is provided to Citcon by, or on behalf of, Customer through Customer’s use of the Services, and any data that third parties submit to Customer through the Services.

“Customer Personal Data” means all Personal Data that is submitted to the Services by or to Customer, processed by Citcon for the purposes of delivering the Services to the Customer including but not limited to the personal data set out in Appendix 2 to this DPA.

“Data Protection Legislations” means:
(i) the General Data Protection Regulation (Regulation (EU) 2016/679)("GDPR") and all other applicable EU, EEA or European single market Member State laws or regulations or any update, amendment or replacement of same that applies to processing of personal data under the Agreement;

(ii) the Swiss Federal Act on Data Protection Act ("FADP"), or the new Federal Act on Data Protection Act that shall come into force on January 1, 2023 ("nFADP");

(iii) all laws and regulations that apply to processing of personal data under the Agreement from time to time in place in the United Kingdom (including the UK GDPR); and

(iv) all U.S. laws and regulations that apply to processing of personal data under the Agreement including but not limited to the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199)("**CCPA**"), as amended by the California Publica Records Act of 2020 (Government Code sections 7920.000 through 7930.215) (“CPRA”);

(v) the Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), or any update, amendment or replacement of same that applies to processing of personal data in Canada.

The terms "controller”, "data protection impact assessment", “process”, “processing”, “processor”, "supervisory authority" have the same meanings as in the GDPR or the UK GDPR.

The terms “Business”, “Business Purpose(s)”, “Commercial Purpose(s)”, “Personal Information”, “Service Provider”, “Sell”, and “Share” have the same meanings as defined in the CCPA.

"Personal Data" means information relating to a living individual who is, or can be, reasonably identified from information, either alone or in conjunction with other information (a "Data Subject").

“Services” means the services ordered by Customer from Citcon under the Agreement.

“SCCs” means the “Standard Contractual Clauses” annexed to the European Commission Decision of: i) 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR or ii) (until such times as Citcon has entered into the Standard Contractual Clauses outlined at i)), the 5 February 2010 for the Transfer of Customer Personal Data to Processors established in Third Countries under Directive 95/46/EC). Where the FADP/nFADP applies, all references made in the SCCs shall be understood as corresponding references to the FADP/nFADP. All terms used in this context shall therefore receive the definition that is provided in the FADP/nFADP.

"UK Addendum" means (i) the template addendum issued by the UK Information Commissioner's Office and laid before the UK Parliament in accordance with section 119A of the UK Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of the Mandatory Clauses from time to time. Where the template addendum referred to in this definition means the document entitled: International Data Transfer Addendum to the EU Commission Standard Contractual, version B1.0, in force 21 March 2022; or (ii) (until such time as Citcon has entered into the UK Addendum outlined at (i)), European Commission Decision of the 5 February 2010 for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

"UK GDPR" means the EU GDPR as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 respectively and any legislation in force in the United Kingdom from time to time that subsequently amends or replaces the UK GDPR.

2. Status of Citcon

In the provision of the Services to the Customer, Citcon is a processor of Customer Personal Data for the purposes of GDPR. Citcon is a Service Provider and Customer is the Business with respect to Personal Information.

3. Term

This DPA shall remain in force until such time as the Agreement is terminated (in accordance with its terms) or expires.

4. Customer's Obligations

Customer shall ensure and hereby warrants and represents that it is entitled to transfer the Customer Data to Citcon so that Citcon may lawfully process and transfer the Personal Data in accordance with this DPA. Customer shall ensure that any relevant data subjects have been informed of such use, processing, and transfer as required by the Data Protection Legislation and that lawful consent have been obtained (where appropriate). Customer shall ensure that any Personal Data Processed or transferred to Citcon will be done lawfully and properly. Customer will comply with all applicable Data Protection Legislations.

5. Citcon's Obligations

Where Citcon is processing Customer Personal Data for Customer as a processor or a service provider, Citcon will:

(a) only do so on documented Customer instructions and in accordance with the Data Protection Legislations, including with regard to transfers of Customer Personal Data to other jurisdictions or an international organization, and the parties agree that the Agreement constitutes such documented instructions of the Customer to Citcon to process Customer Personal Data (including to locations outside of the EEA) along with other reasonable instructions provided by the Customer to Citcon (e.g. via email) where such instructions are consistent with the Agreement;

(b) ensure that all Citcon personnel involved in the processing of Customer Personal Data are subject to confidentiality obligations in respect of the Personal Data;

(c) make available information necessary for Customer to demonstrate compliance with its Article 28 obligations (or similar requirements in the Data Protection Legislations if applicable to the Customer) where such information is held by Citcon and is not otherwise available to Customer through its account and user areas or on websites, provided that Customer provides Citcon with at least 14 days' written notice of such an information request;

(d) co-operate as reasonably requested by Customer to enable Customer to comply with any exercise of rights by a Data Subject afforded to Data Subjects by the Data Protection Legislations in respect of Personal Data processed by Citcon in providing the Services;

(e) provide assistance, where necessary, with requests received directly from a Data Subject in respect of a Data Subject's Personal Data submitted through the Services;

(f) upon losing purpose to process, not retain Customer Personal Data other than in order to comply with applicable laws and regulations and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes subject to our retention policies;

(g) cooperate with any supervisory authority or any replacement or successor body from time to time (or, to the extent required by Customer, any other data protection or privacy regulator under the Data Protection Legislations) in the performance of such supervisory authority's tasks where required;

(h) assist Customer as reasonably required where Customer:

> (i) conducts a data protection impact assessment involving the Services (which may include by provision of documentation to allow customer to conduct their own assessment); or
>
> (ii) is required to notify a Security Incident (as defined below) to a supervisory authority or a relevant Data Subject.

(i) not Sell or Share any Customer Personal Data except to share the Customer Personal Data where it is necessary for the provision of the Services or the compliance of applicable laws and regulations;

(j) not collect, retain, use, disclose, or otherwise process Personal Data other than for the following specific Business and Commercial Purposes: (1) to provide our Services as described in the Agreement; (2) to improve our existing services and develop new services (for example, by conducting research to develop new products or features); (3) for our operational purposes and the operational purposes of our vendors and integration partners; (4) to ensure security and integrity to the extent the use of the data subject’s personal data is reasonably necessary and proportionate for these purposes; (5) Debugging to identify and repair errors that impair existing intended functionality; (6) Short-term, transient use, such as customizing content that we or our vendors display on the services; and (7) other uses that we notify you about as permitted under the Data Protection Legislations;

(k) Citcon shall not retain, use, combine, or disclose the Personal Data collected pursuant to the Agreement outside a direct business relationship between Citcon and Customer, unless expressly permitted by the CCPA and the CPRA;

(l) Where required by the Data Protection Legislations, Citcon will inform Customer if it comes to Citcon's attention that an instructions received from Customer breaches the provisions of the Data Protection Legislations. Notwithstanding the foregoing, Citcon shall have no obligation to monitor or review the lawfulness of any instruction received from Customer. If Citcon makes a determination that it can no longer comply with its obligations under the CCPA or CPRA, Citcon will inform the Customer; and

(m) Citcon certifies that it understands the restrictions and obligations set forth in this DPA and all the applicable Data Protection Legislations and that it will comply with those requirements.

6. Subprocessors

6.1 Customer provides a general authorization to Citcon to engage onward subprocessors, subject to compliance with the requirements in this Section 6.

6.2 Citcon will, subject to the confidentiality provisions of the Agreement or otherwise imposed by Citcon:

(a) make available to Customer a list of the Citcon subcontractors who are involved in processing or subprocessing Customer Personal Data in connection with the provision of the Services ("Subprocessors"), together with a description of the nature of services provided by each Subprocessor upon request.

(b) ensure that all Subprocessors are bound by contractual terms that are in all material respects no less onerous than those contained in this DPA; and

(c) be liable for the acts and omissions of its Subprocessors to the same extent Citcon would be liable if performing the services of each of those Subprocessors directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6.3 Citcon will provide Customer with written notice of the addition of any new Subprocessor or replacement of an existing Subprocessor at any time during the term of the Agreement.

7. Security

7.1 Citcon implements and maintains appropriate technical and organizational security measures that are designed to protect Customer Data from security incidents and designed to preserve the security and confidentiality of Customer Data in accordance with Citcon's Security Safeguards described in Appendix 1 ("Security Measures") of this DPA.

7.2 Citcon ensures that any person who is authorized by Citcon to process Customer Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

7.3 Customer is responsible for reviewing the information made available by Citcon relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under the Data Protection Regulations. Customer acknowledges that

the security measures are subject to technical progress and development and that Citcon may update or modify the Security Safeguards from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Customer.

7.4 If Citcon becomes aware of any unauthorized or unlawful access to, or acquisition, alternation, use, disclosure, or destruction of, Customer Personal Data ("Security Incident"), Citcon will take reasonable steps to notify Customer without an undue delay. A security incident does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems. Any notification of a security incident to Customer does not constitute any acceptance of liability by Citcon.

7.5 Customer responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting data collected from a third party in respect of the Services, protecting the security of Customer Data when in transit to and from the Services, and taking appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

7.6 Citcon will reasonably cooperate with Customer with respect to any investigations relating to a security incident with preparing any required notices, and provide any information reasonably requested by Customer in relation to the security incident.

8. Audits

8.1 Audits. Where Citcon is processing Customer Personal Data for Customer as a processor (only), Customer will provide Citcon with at least one month's prior written notice of any audit request, which may be conducted by Customer or an independent auditor appointed by Customer during reasonable business hours (provided that no person conducting the audit shall be, or shall act on behalf of, a competitor of Citcon) ("Auditor"). The scope of an audit will be as follows:

(a) Customer will only be entitled to conduct an audit once per calendar year unless otherwise legally compelled or required by a regulator with established authority over Customer to perform or facilitate the performance of more than 1 audit in that same year (in which circumstances Customer and Citcon will, in advance of any such audits, agree upon a reasonable reimbursement rate for Citcon's audit expenses).

(b) Citcon agrees, subject to any appropriate and reasonable confidentiality restrictions, to provide evidence of any certifications and compliance standards it maintains and will, on request, make available to Customer an executive summary of Citcon's most recent annual penetration tests, which summary shall include remedial actions taken by Citcon resulting from such penetration tests.

(c) The scope of an audit will be limited to Citcon systems, processes, and documentation relevant to the processing and protection of Customer Personal Data, and auditors will conduct audits subject to any appropriate and reasonable confidentiality restrictions requested by Citcon.

(d) Customer will promptly notify and provide Citcon on a confidential basis with full details regarding any perceived non-compliance or security concerns discovered during the course of an audit.

8.2 The parties agree that, except as otherwise required by order or other binding decree of a supervisory authority or regulator with authority over Customer, this Section 8 sets out the entire scope of the Customer's audit rights as against Citcon.

9. International Data Transfers

9.1 To the extent applicable, for transfers of Customer Personal Data from the European Economic Area ("EEA"), Switzerland, or the United Kingdom to locations outside the EEA, Switzerland, and the United Kingdom (either directly or via onward transfer) that do not have adequate standards of data protection as determined by the European Commission or relevant Data Protection Legislations, Citcon relies upon:

(a) the SCCs; and

(b) for transfers subject to the UK GDPR, the UK Addendum; or

(c) such other appropriate safeguards, or derogations (to the limited extent appropriate), specified or permitted under the Data Protection Legislation.

9.2 Where required, the parties hereby enter into the SCCs (a copy of which is accessible here) and the UK Addendum (Appendix 3). The SCCs are incorporated into this Agreement by reference and shall apply as follows:

(a) where Customer contracts with Citcon in the United States under the Agreement for Services and is a data controller of Customer Personal Data and through use of the Services is transferring that Customer Personal Data from the EEA to locations which have not been determined to provide adequate levels of protection to Personal Data by the European Commission, Citcon enters into the SCCs as data importer and Customer enters into the SCCs as data exporter and Module Two only of the SCCs will apply; and/or

(b) where Customer contracts with Citcon in the United States under the Agreement for Services and is a data processor of Customer Personal Data and through use of the Services is transferring that Customer Personal Data from the EEA to locations which have not been determined to provide adequate levels of protection to Personal Data by the European Commission, Citcon enters into the SCCs as data importer and the Customer enters into the SCCs as data exporter and Module Three only of the SCCs will apply; and/or

(c) in Clause 7, the optional docking clause will not apply;

(d) in Clause 11, the optional language will not apply;

(e) in Clause 17, the SCCs will be governed by Irish law;

(f) in Clause 18, disputes shall be resolved before the courts of Ireland; and

(g) Annex I and II of the SCCs shall be deemed completed with the information set out in the Agreement and details provided in the Appendices to this DPA.

9.3 For transfers that are protected by the FADP/nFADP, the SCCs shall apply in accordance with Section 9.2 above, except:

(a) any references in the SCCs to the GDPR shall be interpreted as references to the FADP/nFADP;

(b) any references to “EU”, “Union”, and “Member State law” shall be interpreted as references to Switzerland and Swiss law; and

(c) any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland, unless the SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the FADP/nFADP, in which case the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. For the purposes of the Swiss SCCs, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in

the Appendices I and II to this DPA (as appropriate) and the interpretive provisions set out in this section 9.3 shall apply (as applicable and as required for the purposes of complying with the FADP/nFADP).

9.4 Upon written request and in accordance with the provisions of the Standard Contractual Clauses or UK Addendum (as applicable), Citcon will provide copies of the Standard Contractual Clauses or UK Addendum that it has entered into with data importers in its capacity as processor to Customer.

10. General Provisions

10.1 Liability for data processing. Each party's aggregate liability for any and all claims whether in contract, tort (including negligence), breach of statutory duty, or otherwise arising out of or in connection with this DPA shall be as set out in the Agreement, unless otherwise agreed in writing by the parties.

10.2 Conflict. In the case of conflict or ambiguity between: (i) the terms of this DPA and the terms of the Agreement, with respect to the subject matter of this DPA, the terms of this DPA shall prevail; (ii) the terms of any provision contained in this DPA and any provision contained in the Standard Contractual Clauses, the provision in the Standard Contractual Clauses shall prevail.

10.3 Independent Processing. Customer remains exclusively liable for its own compliance with Data Protection Legislation with respect to any independent collection and processing of personal data unrelated to the Services. Customer will provide its own clear and conspicuous privacy notices that accurately describe how it does this and Citcon will not be liable for any treatment of personal data by Customer in those circumstances. Customer hereby indemnifies Citcon in full for any and all claims or liability arising as a result of such collection and use of personal data by it in those circumstances.

10.4 Entire Agreement. The Agreement (which incorporates this DPA) represents the entire agreement between the parties and it supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. Each of the parties confirms that it has not relied upon any representations not recorded in the Agreement inducing it to enter into the Agreement.

10.5 Severance. If any provision of this DPA is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed and the remainder of terms will remain in full effect. Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, nor authorize any part to may or enter into any commitments for or on behalf of any other party except as expressly provided herein.

10.6 Governing Law. This DPA shall be governed by the laws of Ireland and the parties submit to the exclusive jurisdiction of the Irish courts (in relation to all contractual and non-contractual disputes) except in the case of any alleged breach or breach of current or future privacy laws, regulation, standards, regulatory guidance, and self-regulatory guidelines at state or federal level in the United States of America, in which case the laws of the State of California shall govern unless otherwise dictated by law.

Appendix 1

Description of the technical and organizational security measures implemented by Citcon

Citcon will maintain appropriate organizational and technical safeguards ("**Security Safeguards**") for protection of the security, confidentiality and integrity of Personal Data provided to it for provision of the Services to the Customer.

The Security Safeguards include the following:

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest. Company uses only recommended secure cipher suites and protocols to encrypt all traffic in transit and Customer Data is securely encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Company's customer agreements contain strict confidentiality obligations. Additionally, Company requires every downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in Company's customer agreements. Company has undergone a SOC 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Daily, weekly and monthly backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Company has undergone a SOC 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for user identification and authorization	Company uses secure access protocols and processes and follows industry best-practices for authentication, including Multifactor Authentication and Single Sign On (SSO). All production access requires the use of two-factor authentication, and network infrastructure is securely configured to vendor and industry best practices to block all unnecessary ports, services, and unauthorized network traffic.
Measures for the protection of data during transmission	Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Company uses only recommended secure cipher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2)

Measures for the protection of data during storage	Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.
Measures for ensuring physical security of locations at which personal data are processed	All Company processing occurs in physical data centers that are managed by AWS. https://aws.amazon.com/compliance/data-center/controls/
Measures for ensuring events logging	Company monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Company adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	Company maintains an SOC 2 compliant risk-based information security governance program. The framework for Company's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.
Measures for certification/assurance of processes and products	Company undergoes annual SOC 2 audits.
Measures for ensuring data minimisation	Company's Customers unilaterally determine what data they route through the Services. As such, Company operates on a shared responsibility model. Company gives Customers control over exactly what data enters the platform. Additionally, Company has built in self-service functionality to the Services that allows Customers to delete and suppress data at their discretion.
Measures for ensuring data quality	Company has a multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) a schema-first API design using GraphQL and strong typing to enforce a strict contract between official clients and API resolvers. Company applies these measures across the board, both to ensure the quality of any Usage Data that Company collects and to ensure that the Company Platform is operating within expected parameters. Company ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data is presented or exported.

Measures for ensuring limited data retention	Customers unilaterally determine what data they route through the Services. As such, Company operates on a shared responsibility model. If a Customer is unable to delete Personal Data via the self-services functionality of the Services, then the Company deletes such Personal Data upon the Customer's written request, within the timeframe specified in this DPA and in accordance with Applicable Data Protection Law. All Personal Data is deleted from the Services following service termination.
Measures for ensuring accountability	Company has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Personal Data Breaches, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, the Company conducts regular third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	Personal Data submitted to the Services by Customer may be deleted by the Customer or at the Customer's request. Personal Data is incidental to the Company's Services. Based on Privacy by Design and Data Minimization principles, Company severely limits the instances of Personal Data collection and processing within the Services. Most use cases for porting Personal Data from Company are not applicable. However, Company will respond to all requests for data porting in order to address Customer needs.
Technical and organizational measures of sub-processors	The Company enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this DPA.

Appendix 2

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Protecting data, including restricting, encrypting, and security testing
- Holding data, including storage, organization, and structuring
- Erasing data, including destruction and deletion
- Analyzing data, including product usage assessment
- Sharing data, including disclosure to subprocessors as permitted in this DPA

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Company Account Data and Company Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects: Customer's employees, consultants, contractors, and/or agents.

Categories of Personal Data: Company processes Personal Data contained in Company Account Data, Company Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include name, email, username, IP address, and financial information.

Sensitive Data or Special Categories of Data: If applicable, transferred sensitive data is subject to stringent safeguards that consider both the data's nature and associated risks. These measures may include strict limitations on the data's use, restricted access only for specially-trained staff, limits on further data sharing, and enhanced security protocols.

Appendix 3

UK ADDENDUM

1. In relation to data transfers that are subject to the UK GDPR, the parties hereby enter into the UK Addendum (a copy of which is accessible here) and the UK Addendum is incorporated into this Agreement by reference. For data transfers that are subject to the UK GDPR, any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in the UK.

2. The parties agree that the format and content of the tables in Part 1 of the UK Addendum shall be amended and replaced with the table below.

UK Addendum Table Reference	Information to complete the table
Table 1: Start Date	Effective as of the Effective Date of the Agreement.
Table 1: Parties' details	Shall be deemed completed with the information set out in Appendix 2 of this Agreement.
Table 2: Addendum EU SCCs	The parties select the following option from Table 2: "Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum". Details of the "modules", "clauses" and "optional provisions" of the SCCs that are brought into effect for the purposes of the UK Addendum are set out above in Section 9.2 of this Agreement.
Table 3: Annex 1A – List of parties	Shall be deemed completed with the information set out in Appendix 2 to this Agreement.
Table 3: Annex 1B – Description of Transfer	Shall be deemed completed with the information set out in Appendix 2 to this Agreement.
Table 3: Annex II – Technical and organizational measures	Shall be deemed completed with the information set out in Appendix 1 to this Agreement.
Table 3: Annex III: List of Sub processors (Modules 2)	A list of subprocessors can be found in accordance with the subprocessor provisions of the Agreement.
Table 4: Ending this Addendum	The parties select that neither party may end the UK Addendum as it is incorporated into the Agreement.

3. In the event of a conflict or inconsistency between this Agreement and the UK Addendum, the UK Addendum controls and take precedence in respect of such conflict or inconsistency.