MASTER SERVICES AGREEMENT

1. PARTIES

1.1. **VTEX Ecommerce Platform Limited**, a company incorporated in England (number 10867517), having its registered office at WeWork Aviation House, 125 Kingsway WC2B 6NH, 6NH, registered under Tax ID (VAT) GB278404189, hereinafter referred to as **"VTEX"** and, **"Customer"** as defined in the commercial proposal set out in Appendix 1, have entered in to this master services agreement and Appendix 1 (together, the **"Agreement"**).

2. OBJECT

2.1. **VTEX** shall provide the **Customer** with the services set out in **Appendix 1** ("**Services**"), and other appendixes, if applicable.

3. PRICE AND PAYMENT CONDITIONS

3.1. In consideration of the provision of the **Services**, the **Customer** shall pay **VTEX** the fees set out in **Appendix 1**. The payment terms and conditions are set out in **Appendix 1**.

4. CUSTOMER'S OBLIGATIONS

4.1. Without prejudice to the other obligations provided for in this **Agreement**, the **Customer** shall:

4.1.1. make the payments due under this **Agreement** in a timely manner, in accordance with the provisions of clause 3 and **Appendix 1**;

4.1.2. inform **VTEX** about any changes to its registration data. The absence of communication will result in **VTEX** validly using the data initially provided;

4.1.3. keep the "Contacts" tab in the billing module on the **VTEX Platform** updated with its financial contacts.

4.1.4. make its best efforts to quickly respond to all contacts made by **VTEX** to the **Customer** through the tickets opened on the **VTEX Platform** or other contact channels.

4.1.5. manage the operation of the **Services** provided by **VTEX** for e-commerce solutions ("**VTEX Platform**") and manage the launch and maintenance of the **Customer**'s online store through the administrative module provided by **VTEX**, as well as be responsible for the actions of those with whom the **Customer** share access directly or via Sponsor User to this module and/or for any and all persons who may have access to the administration password of the **VTEX Platform** and of any other service that may interfere with the **Customer**'s online store;

4.1.6. Be liable, exclusively and fully, for the activities of its responsibility or of its

subcontractors and representatives, performed in the **VTEX Platform** through the use of the Services, such as the quality and origin of the products and services commercialized; any configuration in the **VTEX Platform** requested by the Customer or third parties acting on the **Customer**'s behalf, even if subject to consultation to **VTEX**; exempting **VTEX** of any responsibility in these regards.

4.1.7. The **Customer** agrees that all orders generated involving any **VTEX Platform** Application Programming Interface ("**API**") must be registered in the **VTEX Platform**'s Order Management System ("**OMS**"). Violation of this provision will be considered a fraudulent use of the **VTEX Platform**.

4.1.8. Grant access to the **VTEX Platform** only to users that must have access to perform the activities object of this **Agreement**, as well as to be responsible for the activities performed with the **VTEX Platform** by all users to whom it has granted access, including the Sponsor User provided in **Appendix 1**. The **Customer** agrees that it will be solely and exclusively responsible for the use and operation of the **VTEX Platform**, including, but not limited to, any and all customizations, functionalities and features added to the **VTEX Platform**. The **Customer** further agrees that **VTEX** will not be liable for any breach of the **SLA** and security vulnerabilities, which has been caused as a result of the implementation or operation of such features and/or customizations.

4.1.9. **Customer** hereby declares that, provided that **VTEX** has a substantially similar Certified APP, Customer shall not integrate **VTEX Platform** with partners who do not provide Certified APPs.

4.1.9.1. In case a substantially similar Certified APP is not available, and the **Customer** still wishes to integrate it into the **VTEX Platform**, the Customer agrees that **VTEX** shall have no liability for any breaches to the **SLA** or any losses and damages that may arise out of or relate to such integration or use of the non-Certified APP.

4.1.9.2. Certified App means an application developed by a **VTEX** partner that has been duly homologated following the process available at: https://developers.vtex.com/vtex-developer-docs/changelog/homologation-requirements-for-the-vtex-app-store.

4.1.10. The **Customer** will not, during the **Term** or after the termination or expiration of this **Agreement**, make disparaging statements, in any form, about **VTEX**, **VTEX**'s officers, directors, agents, employees, the terms of this **Agreement**, its products or **Services**.

4.1.11. Customer shall not use the **VTEX Platform** to: (i) display or transmit pornographic material of any kind; (ii) transmit material that is unlawful, misleading, harassing, libelous, abusive, fraudulent, threatening, harmful, grossly offensive or otherwise objectionable; (iii) transmit material that contains viruses or any other harmful programs or code; (iv) collect, post or distribute personal information about others without their consent; (v) transmit chain letters or any unsolicited e-mail or other electronic messages ("**SPAM**"); (vii) post or transmit any material that may infringe the copyright, trademark, trade dress or other intellectual property rights or any other personal or property rights of a third party; (viii) store files not related to

Customer's web site; (ix) attempt to hack or penetrate security measures; or (x) offer or conduct activities related to gambling, sweepstakes, raffles, lotteries, pyramid or similar schemes; (xi) create an anonymous gateway; and/or (xii) violate any federal, state or local law or regulation of a governing body.

4.1.12. The **Customer** acknowledges that by initiating access to the **VTEX Platform**, all modules of the Master Data (end-user database solution) will be inaccessible to external access. If the **Customer** publishes the Master Data for external integrations and views, the **Customer** will be solely and fully liable for losses and damages, including, but not limited to, those resulting from data leaks occurring in the **VTEX Platform**, and will hold **VTEX** harmless from any related liability to third parties. The **Customer** further understands that the use of encryption is the most appropriate method for protecting information, and it agrees to use it whenever possible.

4.1.13. The **Customer** shall keep its application keys in the expected security of the market during the **Term** of the **Agreement**, shall not perform any public disclosure and shall prevent them from any unauthorized access. In addition, the **Customer** undertakes to periodically renew the application keys during the **Term** of the **Agreement**.

5. VTEX'S OBLIGATIONS

5.1. VTEX shall:

5.1.1. Provide the **Services** in accordance with applicable law.

5.1.2. Ensure that all licenses required to perform the Services under this Agreement are valid and in accordance with applicable law.

5.1.3. **VTEX** may make available beta services, i.e., new services or functionalities in the testing phase of the **VTEX Platform** that may be made available for the Customer to perform tests at its discretion ("**Beta Services**"). Any use of the **Beta Services** will be subject to the specific terms for such utility, to be entered into between the **Parties**.

5.1.4. Use commercially reasonable efforts to provide the **Services**, including the processing infrastructure necessary for the **VTEX Platform**, in accordance with clause 6 of this **Agreement**.

5.1.5. Keep the hosting infrastructure up-to-date with programs to protect against criminal or irregular actions by third parties.

5.1.6. **VTEX** will not, during the **Term** or after the termination or expiration of this **Agreement**, make disparaging statements, in any form, about the Customer, the **Customer**'s officers, directors, agents, employees, the terms of this **Agreement**, the **Customer**'s products or services.

5.1.7. **VTEX** will not be responsible for data and information violations or vulnerabilities resulting from acts, integrations or customizations carried out by employees, agents or persons authorized by the **Customer** to operate the VTEX Platform,

including vulnerabilities due to the absence of application keys updates by the **Customer**.

5.1.8. **VTEX** shall keep the PCI certification (or any other that may replace it) active and up to date throughout the course of the Agreement, which may be consulted by the **Customer** at any time at https://vtex.com/us-en/compliance/certifications/.

6. SERVICE LEVEL (SLA)

6.1. Provided that the **Customer's** obligations are observed and fulfilled under this **Agreement, VTEX** will make commercially reasonable efforts to maintain the **VTEX Platform** operational and live according to a minimum percentage of monthly availability time of 99.7% ("**SLA**"). The calculated period **SLA** of the **VTEX Platform** ("**Calculated SLA**") is calculated considering the total minutes of the month, subtracting the sum of eventual unavailabilities that occurred in the same period.

6.1.1. "**Unavailable**" and "**Unavailability**" means that the **VTEX Platform** is inaccessible to all prospective end clients of the Customer, including all the all accounts linked to it or, in the case of the Platform's Administrative Environment, that it is inaccessible to all the Customer's Sponsor Users.

6.2. In the event of non-compliance with the **SLA**, a credit will be granted to the **Customer** ("**Service Credits**"), calculated by applying a percentage on the monthly fee paid by the **Customer** in the month of occurrence of non-compliance with the **SLA** contracted according to the table below:

Calculated SLA	Service Credits Percentage
Between 0.01% contracted plan and 1.00% below the SLA for the contracted plan	10%
Greater than 1.00% below the SLA for the contracted plan	20%

6.2.1. **Service Credits** will only be granted if, at the time of the opening of the case, the Customer has paid all outstanding invoices. **Service Credits** will only be granted for future payments due by the **Customer** under this **Agreement**. **Service Credits** cannot be transferred or credited to any other agreement. The sole remedy for the **Customer** in relation to any **Unavailability** of the **VTEX Platform** will be the receipt of the **Service Credits**. The **Customer** and **VTEX** acknowledge that the Service Credits are a reasonable pre-estimate of the losses that the **Customer** may suffer as a result of, or in connection with, any Unavailability of the **VTEX Platform**.

6.2.2. To receive **Service Credits**, the **Customer** must open a call through the **VTEX** service system. The request must be received by the last day of the month following the month of unavailability. If the **Calculated SLA** in such a request is lower than the contracted **SLA**, **VTEX** will grant the **Service Credits** in the invoice for the month following the one in which the occurrence was determined.

6.3. The following events are excluded from the **SLA** calculation:

6.3.1. failures in making online sales and/or overloading the hosting infrastructure due to changes in the settings of the **VTEX Platform** under the responsibility of the **Customer** or of a third party contracted by it, including VTEX IO applications developed by third parties or customizations to its store that are not originally available on the VTEX Platform;

6.3.2. In the event of any interruptions necessary for making technical adjustments or maintaining the **VTEX Platform**, **VTEX** shall use reasonable efforts to provide advance notice in writing of not less than 48 (forty-eight) hours. In general, scheduled maintenance does not impact the sales flow of VTEX customers, but it may cause a higher latency than normally practiced. VTEX always seeks to make these scheduled maintenances in periods of lower access, aiming to impact the sales of its customers as little as possible;

6.3.3. In case of any emergency interventions arising from the need to preserve the security of the VTEX Platform, intended to prevent or impede the action of hackers or to implement emergency solutions and security for the VTEX Platform, VTEX will have no obligation to inform the Customer in advance about such interruptions. These are situations that put at risk to the regular operation of the VTEX Platform, and such interruptions aim to ensure the security of all users in the face of detected vulnerabilities, including, but not limited to: (i) Zero Day Vulnerabilities, (ii) DDoS attacks, (iii) exploitation of vulnerabilities with access to information systems and (iv) Ransomware attacks;

6.3.4. when carrying out any emergency interventions arising from the need to preserve the security of the **VTEX Platform**, aimed at preventing or stopping the work of hackers, or aimed at implementing emergency and security corrections for the **VTEX Platform**;

6.3.5. suspension of the provision of the **Services** (i) by determination of a competent authority; (ii) due to non-compliance by the **Customer** of any clause of this **Agreement**; or (iii) receipt of a notification alleging that the Customer infringes third-party intellectual property rights;

6.3.5.1. VTEX will notify the Customer in case of receipt of a notification and the Customer will be given 2 days to comply with the established requirements;

6.3.6. if the maximum daily limit of visitors accessing the **VTEX Platform** is exceeded, which shall correspond to twice the daily average of visitors of the last 60 (sixty) days, provided that the **Customer** has not communicated to **VTEX**, at least 72 (seventy-two) hours in advance, of any circumstance that may subject the **VTEX Platform** to an unusual demand load. Although the VTEX Platform is auto-scalable, if the number of accesses suddenly increases without VTEX having been notified of this trend and having prepared for this increase in accesses, there may be a risk of instability in the VTEX Platform;

6.3.7. cases of overload, **Unavailability** or slowness caused by the **Customer** or third party contracted by it via *WebService* (**API**), data import through the administrative environment, consultations external to its own services or third parties to the **VTEX** system. In this case, if necessary, **VTEX** may temporarily suspend the **Services**. An information flow 10 (ten) times greater than the average verified in the fifteen

days prior to the occurrence will be considered overload; and

6.3.8. instabilities of software and services outside of VTEX´s control, such as, without limitation, disruptions on core telecom network or on public cloud provider's core services.

7. VTEX LIMITATION OF LIABILITY

7.1. **VTEX** shall not have any liability, whether arising out of breach of contract, tort (including negligence), breach of statutory duty, misrepresentation (whether innocent or negligent), restitution or otherwise, for direct, indirect, consequential, or special losses, loss of profits, business, business opportunities, revenue, turnover, reputation or goodwill, loss or corruption of data or information, loss of anticipated savings or wasted expenditure, regardless of any notice.

7.2. For exemplification purposes only, VTEX will not be liable for:

7.2.1. Damages and losses resulting from
(i) the activities carried out by **the Customer** on the **VTEX Platform;** or
(ii) the content produced by the **Customer** on the **VTEX Platform**;

7.2.2. errors and/or interruptions in the **Services** caused by the use of the **VTEX Platform** combined with *software* or in conjunction with components, interfaces, *hardware* and/or environments not provided by **VTEX**;

7.2.3. losses arising from **Force Majeure Event** as set out in clause 13 of this **Agreement**;

7.2.4. violations of data or information resulting from

(i) acts of employees, agents, or persons authorized by the **Customer** to operate the **VTEX Platform**, or

(ii) criminal or irregular actions by third parties that cannot be avoided because they are outside the limits of predictability when they occur;

7.2.5. any inability of the **Customer** to use the **Services** as a result of
(i) termination or suspension of this Agre**ement**;
(ii) discontinuation, by **VTEX**, of some functionalities of the **VTEX Platform**; and
(iii) requests for services that are not the obligation of **VTEX**;

7.2.6. any investments, expenditures, or commitments assumed by the **Customer** in relation to this **Agreement** or with the use by the **Customer** of the **Services**; and

7.2.7. Damages arising from activities practiced in the VTEX Platform as a result of any access granted and authorized by the Customer to the VTEX Platform, as well as the modification, deletion, destruction, damage, loss or failure to store any of its content or data by the Customer or any user to whom the Customer may have given access.

7.3. Without prejudice to the exclusions provided in sections 7.1 and 7.2 above, **VTEX**'s total aggregate liability under or in connection with this **Agreement**, whether or not foreseeable or in

the contemplation of the parties and whether arising out of breach of contract, tort (including negligence), breach of statutory duty, misrepresentation (whether innocent or negligent), restitution or otherwise, will be limited to 10% (ten percent) of the total amount paid by the **Customer** to **VTEX**, in accordance with the provisions of **Appendix 1**, during the 12 (twelve) months immediately preceding notice of the loss suffered by the **Customer**. If there is more than 1 (one) claim during the 12 (twelve) months immediately preceding notice of the loss suffered by the **Customer**, the claims will be amalgamated but limited to 10% (ten percent) of the total amount paid by the **Customer** to **VTEX** during such period, in accordance with the provisions of **Appendix 1**.

7.4. For clarification purposes, the limitation of liability provided for in clause 7.3 in no way shall be understood as a limitation of the Customer's rights to the Service Credits provided for in clause 6.4.

8. INTELLECTUAL PROPERTY

8.1. **VTEX** owns all intellectual property rights over the **VTEX Platform**, including, without limitation, eventual developments, new functionalities, and improvements done based on comments and suggestions of the **Customer** or any other clients.This **Agreement** only authorises the use of the **Services** by the **Customer**. **VTEX** warrants that it has the necessary rights to authorize the use of the **VTEX Platform** by the **Customer**. The **Customer** cannot modify or remove any **VTEX** trademark, or **VTEX** trade name, from the places where it appears on the **VTEX Platform**. No provision in this **Agreement** shall be deemed to have granted any right to the **Customer** over the **VTEX** trademark or **VTEX** trade name.

8.2. The **Customer** may not seek to register any trademark or trade name that may cause confusion with **VTEX**'s trademark or trade name.

8.3. The **Customer** may store data in the database of the **VTEX Platform**. Such data is the sole and exclusive property of the **Customer**, and the **Customer** authorises **VTEX** to anonymise the **Customer's** data and use the data in an anonymised form to help improve **VTEX's** products and services. The aggregated anonymous data set can be used to activate features such as benchmarks and publications that can help understand data trends, as well as assist **VTEX** in sizing its infrastructure.

8.4. Parties authorize each other to use their trademark, and logo to publicize the launch of the **Customer**'s online store. Parties agree to participate in two recorded interviews per year, reporting their successful partnership. Such recordings may be published by either Party, subject to each other's consent - that shall not be unreasonably withheld. Silence by either Party for more than 7 (seven) business days shall be considered approval for publishing. The **Customer** shall include **VTEX**'s logo and hyperlink in the footer of its online store frontend.

8.5. VTEX grants Customer a worldwide, non-exclusive, non-sublicensable, non-transferable, license to use one copy of the VTEX Platform ("Software"), in object code format, solely for the purposes of the Agreement. The Customer may not reverse-engineer, decompile, or disassemble the Software, or otherwise reduce the code of the Software, except if that restriction is prohibited by applicable law, and in such event, Customer shall provide VTEX prompt notification of such activities.

8.5.1. In case of violation of section 8.5, VTEX can terminate this Agreement upon prior notice of 48 hours, without prejudice to the payment by Customer of any losses and damages suffered by VTEX arising from such violation.

8.6. Upon termination of this Agreement, all use of the Software must cease, and Customer hereby agrees to return to VTEX or to destroy all copies of the Software in its possession or control within thirty (30) days of such termination.

9. TERM AND TERMINATION

9.1. This **Agreement** will become effective on the date of signature of Appendix 1 and will remain in effect for the term set forth in Appendix 1 ("Term"). Unless otherwise defined, the Agreement shall be automatically extended for additional periods equal to the Term, and so on, unless either Party gives the other ninety (90) days prior written notice of its intention not to renew the Agreement.

9.2. VTEX may, at its sole discretion and at any time, immediately terminate this **Agreement** if:

9.2.1. it reasonably believes that the **Customer** is not using the **Services** strictly in accordance with this **Agreement** and with **VTEX**'s standard published policies (https://compliance.vtex.com), or if the **Customer** is using spam (sending e-mail or any other type of unauthorised electronic message to carry out unsolicited advertising, or for any other purpose, which may give rise to a complaint by its recipients);

9.2.2. the **Customer** fails to make payment in accordance with this Agre**ement** and does not remedy that failure after being given ten (10) days' written notice requiring it to make payment; or

9.2.3. the **Customer** challenges, directly or indirectly, itself or in collaboration with third parties, **VTEX**'s trademark or trade name or its related registrations.

9.3. Either Party may terminate this **Agreement** if the other party commits any material breach of its obligations under this **Agreement**:

9.3.1. in the case of a material breach which is capable of remedy, the other Party fails to remedy it after being given fifteen (15) days' written notice specifying the breach and requiring it to be remedied; or

9.3.2. in the case of a material breach which is incapable of remedy, immediately by notice in writing to the other **Party**.

9.4. VTEX may suspend the **Services** temporarily and immediately in the event that it receives a notification alleging that the **Customer**'s content violates or infringes the intellectual property rights of third parties, without said suspension implying any payment or compensation to the **Customer** or counting for the calculation of the **SLA**, according to clause 6.3.4.

9.5. The termination or expiry of this **Agreement** does not affect any right or remedy that has accrued prior to the date of termination, including payment by the **Customer** of any installment due in respect of **Services** provided by **VTEX**, provided that **VTEX** has effectively rendered the **Services**.

9.6. This **Agreement** may also be immediately terminated by either **Party**, for a just cause and regardless of any judicial or extrajudicial notices, in the event of (i) impossibility of continuing to perform the **Agreement** as a result of legal or regulatory prohibition; or (ii) bankruptcy, judicial or extrajudicial recovery, dissolution or judicial or extrajudicial liquidation of any of the **Parties**, requested or ratified.

9.7. **VTEX** may terminate the **Agreement**, without being subject to any penalty or compensation, upon giving the Customer at least 150 days' notice.

10. DEMANDS FROM THIRD PARTIES

10.1. The **Customer** acknowledges that **VTEX** has no control over the products or content displayed on the **VTEX Platform** and it warrants that if it receives a warning, including from **VTEX**, that content or an uncertified APP may no longer be used or must be removed, modified and/or disabled to avoid violation of applicable law or third party rights, it will do so promptly. If the Customer fails to take necessary action, **VTEX** may disable such content, product, service and/or uncertified APP. If requested by **VTEX**, the **Customer** shall confirm the deletion and discontinuance of such use in writing and **VTEX** shall be authorized to provide a copy of such confirmation to any complainant or governmental authority, as applicable.

11. COMPLIANCE COMMITMENT

11.1. The Parties declare to have full knowledge of the VTEX's Code of Ethics and Conduct for Third Parties ("Code of Ethics") available at https://vtex.com/us-en/compliance/ethics/ and the Anti-Corruption and Anti-Money Laundering Policies available at https://vtex.com/us-en/compliance/policies-and-procedures/ and undertakes to observe for itself, its administrators, agents, representatives, and employees, as applicable, its principles and guidelines, maintaining, throughout their relationship with each other, the highest standards of ethics and integrity.

11.2. Any breach of the obligations contained in Clause 11 or any applicable anti-corruption law will be considered a violation of this instrument that cannot be corrected or remedied, and the Party not involved in the breach may declare this Agreement terminated for just cause and with immediate effect, regardless of any notice.

12. CONFIDENTIALITY

12.1. All information disclosed by a party ("**Disclosing Party**") to another party ("**Receiving Party**") as a result of the **Services**, before or after the execution of this Agre**ement**, by any means, including, without limitation, information related to technology, technical or scientific data, plans, strategies, predictions, know-how, trade secrets, research, products, services, inventions (patentable or not), ideas, materials, processes, design, drawings, schemes, models, samples, computer programs, names and data of customers, employees or suppliers, as well as other tangible or intangible forms of information, regardless of whether such information is identified or not, will be hereinafter referred to as "**Confidential Information**". **Confidential Information** excludes any information which: (i) is required to be disclosed by law, by order of any court or by any government agency; (ii) that is or becomes publicly known other than through a breach of this **Agreement**; (iii) is independently developed by the **Receiving Party** and that independent development can be shown by written evidence; (iv) is lawfully disclosed to the **Receiving Party**

by a third party without restriction or disclosure; or (v) was in the **Receiving Party's** lawful possession before the disclosure.

12.2. The **Receiving Party** agrees to: (i) treat **Confidential Information** with, at least, the same degree of care with which it treats its own **Confidential Information**; (ii) notify the **Disclosing Party** immediately and in writing of any misuse or misappropriation of **Confidential Information** of which it becomes aware; and (iii) use **Confidential Information** exclusively for the purposes of discussing, evaluating and performing the **Services**.

12.3. **VTEX** may disclose **the Customer's Confidential Information** to its employees, agents, affiliates, and subcontractors who need to be aware of the **Confidential Information** to perform the obligations contained in this **Agreement**, provided such persons are subject to confidentiality obligations that are no less onerous than the terms of this **Agreement**, and the **Customer** must do the same in relation to **VTEX's Confidential Information** with respect to its employees and third parties. Each **Party** assumes full responsibility for the acts and omissions of its Customers and employees that breach this clause.

12.4. The **Receiving Party** shall return to the **Disclosing Party** or destroy, at the sole discretion of the **Disclosing Party**, all **Confidential Information**, any copies (such as backing up information for archival purposes), and all documents and materials containing any part of the **Confidential Information**, as well as cease and ensure that its employees cease the use of **Confidential Information**, immediately after the termination or expiration of this **Agreement** or upon written request from the **Disclosing Party** to this effect. Notwithstanding the destruction or return of **Confidential Information**, the **Receiving Party** will continue to be bound by its obligations under this **Agreement**.

12.5. The parties recognise that the breach or omission of the respective obligations resulting from this clause may cause immediate and irreparable damage to the other party that cannot be adequately compensated and that, in the eventual breach or omission and in addition to all other legal or equity solutions, the affected party shall have the right to request preventive measures from any competent court or jurisdiction, without the need to prove actual damage or collateral or other security.

12.6. This clause 11 shall survive 5 (five) years after termination of this **Agreement**.

13. PROTECTION OF PERSONAL DATA AND SECURITY

13.1. To the extent that **VTEX** processes any **Customer Personal Data** in the course of providing the **Services**, the parties shall comply with their obligations under the VTEX Data Processing Addendum (https://compliance.vtex.com) executed by the **Parties** on or about the date of this **Agreement**.

13.2. The Customer can only perform any type of penetration test ("pentest") or vulnerability scan on the VTEX Platform if previously authorized by VTEX and upon compliance with the pre-established procedure for requesting security tests. No third party is authorized to perform such tests. Any results or reports of vulnerability scans or pentests conducted by the Customer or any third party acting on the Customer's behalf will belong exclusively to VTEX. In no event will VTEX be responsible for any costs related to penetration tests performed by the Customer.

14. **VTEX** may immediately limit access, partially or totally, to the **Customer**'s **VTEX Platform** environment, if a **Security Incident** occurs in its environment, in order to maintain the security of

the **VTEX Platform**. After the limitation, **VTEX** shall send, within 24 (twenty-four) business hours, documents proving the identification of the security incident to the **Customer**, with VTEX not being responsible for any consequences of such limitation, being applicable the clauses of limitation of liability set forth in this **Agreement**.

14.1. "Security Incident" means any explicit attack and/or a violation of standard security practices that may impair the availability of the **Services**, the integrity of **VTEX**'s or **Customer**'s computers and applications of the **Parties**, data privacy and/or or **VTEX** property and may be reported by monitoring employees, partners and external parties.

15. FORCE MAJEURE

15.1. Except for the **Customer's** obligation to make payment, neither party shall be in breach of this **Agreement** or otherwise liable for any delay or failure to perform obligations under this **Agreement** if the delay or failure results from a **Force Majeure Event**. In such circumstances, either party may rely on the provisions of this clause 13 for exemption from liability for non-performance part performance defective performance or delay, and in the event that any such delay or failure continues for a period in excess of 90 consecutive days, either party shall have the right to terminate this Agre**ement** with immediate effect by giving notice in writing to the other party.

15.2. "**Force Majeure Event**" means any circumstance not within a party's reasonable control including, without limitation (a) acts of God, flood, drought, earthquake or other natural disaster; (b) epidemic or pandemic; (c) terrorist attack, civil war, civil commotion or riots, war, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, or breaking off of diplomatic relations; (d) nuclear, chemical or biological contamination or sonic boom or pandemic; (e) any law or any action taken by a government or public authority, including without limitation imposing an export or import restriction, quota or prohibition, or failing to grant a necessary licence or consent; (f) collapse of buildings, fire, explosion or accident; (g) any labour or trade dispute, strikes, industrial action or lockouts (other than in each case by the party seeking to rely on this clause, or companies in the same group as that party); (h) non-performance by suppliers or subCustomers (other than by companies in the same group as the party seeking to rely on this clause), such as, without limitation, an outage on AWS´s services; and (i) interruption or failure of utility service.

16. GENERAL PROVISIONS

16.1. This **Agreement** constitutes the entire agreement between the **Parties** and supersedes any previous agreement, arrangement, or understanding (whether oral or written) between the parties relating to its subject matter.

16.2. Each **Party** agrees that in entering into this **Agreement**, all statements, representations, warranties, and undertakings on which it relies are incorporated into this **Agreement** and it does not rely on (and shall have no remedy in respect of) any statement, representation (including any misrepresentation), warranty or undertaking (whether negligently or innocently made) of any person (whether **Party** to this **Agreement** or not) (in each case whether contractual or non-contractual) which is not expressly set out in this **Agreement**. Without prejudice to any other provision of this **Agreement** limiting the remedies available to either **Party**, each **Party** agrees that it will have no remedy in relation to this **Agreement** for innocent or negligent misrepresentation, negligent misstatement, or mistake based on any statement in or made in relation to this **Agreement**. Without prejudice to any **Party's** ability to seek injunctive or

equitable relief, the only remedy available to each **Party** in relation to any breach of this **Agreement** shall be for damages for breach of contract under the terms of this **Agreement**.

16.3. No variation of this **Agreement** shall be effective unless it is in writing and signed by both parties. In the event of inconsistency or ambiguity between the main body of this **Agreement** and **Appendix 1**, the terms set out in **Appendix 1** shall prevail.

16.4. If any provision (or part of a provision) of this **Agreement** is found to be invalid, unenforceable, or illegal, the other provisions (or parts of any provisions) will remain in force. If any provision or part-provision of this **Agreement** is deemed deleted under this Clause, the **Parties** shall negotiate in good faith to agree on a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

16.5. A person who is not a **Party** to this **Agreement** shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this **Agreement**.

16.6. Except as expressly provided in this **Agreement**, the rights, and remedies provided under this Agre**ement** are in addition to, and not exclusive of, any rights or remedies provided by law.

16.7. The fact that any of the parties fail to exercise, or delays in the exercise of, any right or remedy under this **Agreement** will not be considered a waiver of that or any other right or remedy, and nor shall it preclude or restrict the **further** exercise of that or any other right or remedy or affect the validity of this **Agreement**. No single or partial exercise of any right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

16.8. The **Customer** may not transfer, assign, charge, sub-contract, declare a trust over, or deal in any other manner, in whole or in part, with all or any of its rights and obligations under this **Agreement** to third parties without the written consent of **VTEX**.

16.9. The **Customer** hereby authorises **VTEX** to share the **Customer**'s data with **VTEX**'s partners for the purpose of developing the **Services**.

16.10. This **Agreement** is signed on a non-exclusive basis and, therefore, the parties are free to enter into similar contracts with third parties or any other type of **Agreement** with the same purpose and object.

16.11. All notices under this **Agreement** must be made in writing and will be deemed delivered to the recipient:

16.11.1. if delivered by hand, at the time of delivery;

16.11.2. if sent by means of an internationally recognised courier, at 4.30 pm on the third business day following dispatch; or

16.11.3. if sent by email, upon receipt confirmation, provided that a copy of the notice is also sent to the recipient in accordance with clauses 14.11.1 or 14.11.2.

16.12. The parties declare and guarantee that they know and understand the anti-corruption laws, committing themselves to (i) not perform acts harmful to the national or foreign public administration, as well as refraining from promising, offering, giving, directly or indirectly, by itself

or by an interposed third party, undue advantage to a national or foreign public agent, or the third person related to it; (ii) implement adequate guidelines and controls aimed at preventing and correcting deviations, in order to comply with and ensure that its administrators, employees, Customers and other representatives comply with the provisions of the anti-corruption laws; and (iii) evidence, at the request of the other party, the effectiveness of these guidelines and controls.

16.13. The **Customer** shall insert the **VTEX** signature ("Powered by VTEX"), in the form of its logo containing a hyperlink to its website, in all items accessible to users of the **VTEX Platform**.

16.14. **VTEX** is performing the **Services** as an independent Customer, is not an employee, joint venturer or partner of the **Customer**. No **Party** shall have authority to make any representation for or act as agent for, in the name of or on behalf of another **Party** in any way.

16.15. This **Agreement** may be executed in any number of counterparts and by the Parties hereto in separate counterparts, each of which when so executed shall be deemed to be an original and all of which taken together shall constitute one and the same agreement.

16.16. The Parties may include VTEX international entities and Customer international entities to this Agreement by signing a Territorial Expansion Addendum. The Parties agree that as of the date of execution of the Territorial Expansion Addendum the entities shall observe, comply with, and be bound by the provisions of this Agreement as if such entity were an original party to the Agreement, except for the variations set forth in such Addendum. Each Territorial Expansion Addendum shall be considered a separate and binding agreement between the Parties.

16.17. The rights under this **Agreement** may not be transferred or assigned, in whole or in part, except by mutual written agreement between the **Parties**. Notwithstanding the foregoing, **VTEX** is entitled to assign the billing obligations under this **Agreement** to one of its operational holdings, in which case, no prior approval is necessary.

17. GOVERNING LAW AND ARBITRATION

17.1. This **Agreement** and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed and interpreted in accordance with the laws of England.

17.2. Disputes or claims, including any question regarding their existence, validity or termination, shall be referred to and finally resolved by arbitration under the then applicable Rules (the "Rules") of the London Court of International Arbitration (the "**LCIA**"), which Rules are deemed to be incorporated by reference into this clause, subject to the additional terms below.

17.2.1. The appointment and number of arbitrators shall be made and determined in accordance with the Rules. The seat, or legal place, of arbitration shall be London.

17.2.2. The language to be used in the arbitration shall be English.

17.2.3. Unless the parties to the dispute agree otherwise, no **Party** shall be required to give general discovery of documents, but may be required only to produce specific, identified documents that are relevant to the dispute.

17.2.4. In the event multiple disputes arise and such disputes are of the type that are

subject to resolution by arbitration under this clause, then, upon the request of any **Party**, such disputes shall be consolidated into one arbitration proceeding to the greatest extent possible.

17.3. Notwithstanding the foregoing, nothing in this clause 15 shall prevent a **Party** from pursuing the following matters outside of the arbitration process:

17.3.1. obtaining injunctive relief to prevent the unauthorised use of intellectual property rights or Confidential Information;

17.3.2. suspending the provision to the Customer of all or a part of the Services due to the failure of the

Customer to make all payments as and when required pursuant to the terms of this **Agreement**; or

17.3.3. pursuing amounts which are due and owing to **VTEX** and/or its Affiliates under this **Agreement** through litigation or other judicial process or other means of lawful debt collection that may be permitted in any jurisdiction in which the **Customer** is located or in which **VTEX** and its Affiliates providing the **Services** are located.

Location, date and signatures on Appendix 1

Appendix 2
Data Processing Terms

This Section includes certain details of the processing of **Customer Personal Data** as required by Article 28(3) **GDPR**: **Subject matter and duration of the processing of the Personal Data.** The subject matter and duration of the
Processing of the **Customer Personal Data** are as set out in this Agre**ement**.

The nature and purpose of the processing of the Personal Data. The nature and purpose of the **Processing** of the
Customer Personal Data are as set out in this Agre**ement**.

The categories of Data Subject to whom the Customer Personal Data relates. The categories of **Data Subject**
may include some or all of the following:

- Please consult our Data Processing Addendum (https://compliance.vtex.com)

The types of **Customer Personal Data** to be processed. The **Customer Personal Data Processed** may include some or all of the following attributes:

- Please consult our Data Processing Addendum (https://compliance.vtex.com)

The obligations and rights of the **Customer**. The obligations and rights of the **Customer** are as set out in this Agre**ement**.

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Master Services Agreement found at https://vtex.com/us-en/agreements/, unless the Contractor has entered into a superseding written Master Services Agreement with VTEX, in which case, it forms a part of such written agreement. Together, the Master Services Agreement and the Order Form - Commercial Proposal, are referred to as the "**Agreement**".
For the purposes of this DPA only, and except where indicated otherwise, the term "Contractor" shall include the Contractor and those Contractor Affiliates required by the applicable Data Protection Laws to enter into a DPA with VTEX. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.
By signing this addendum, the Contractor enters into this DPA on behalf of itself and, to the extent that the applicable Data Protection Laws require so, on behalf of any Contractor Affiliate (as defined below) that is a third-party beneficiary under the Agreement.
In the course of providing the Services under the Agreement, VTEX may Process certain Personal Data (such terms defined below) on behalf of Contractor and where VTEX Processes such Personal Data on behalf of Contractor the Parties agree to comply with the terms and conditions in this DPA in connection with such Processing of Personal Data.

HOW TO EXECUTE THIS DPA?

1. This DPA consists of two parts: the main body of the DPA, and its five appendices and Appendix):
   - **Appendix 1: Description of the Processing:** Appendix 1 sets out certain information regarding the conditions of Processing resulting from the Services provided by VTEX under the Agreement. Depending on the nature of the data transferred (EU Restricted Transfer or UK Restricted Transfer), such information may serve as a basis to pre-populate Appendix I of the UK Data Processing Addendum.
   - **Appendix 2: Technical and organisational Measures**
   - **Appendix 3: EU Standard Contractual Clauses (Module 2) to be used globally**
   - **Appendix 4: International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**

2. The Data Protection Laws (as defined below) in certain jurisdictions may require the obligations in this DPA and its Appendixes to be supplemented by additional or alternative provisions to ensure the compliance with the respective Data Protection Laws ("Special Terms"). The provisions of this DPA shall also be interpreted in accordance with any Special Terms identified in Exhibit A as applicable to the respective jurisdiction.

3. The Contractor declares to be aware of the clauses foreseen in this DPA when signing the Order Form - Commercial Proposal.

HOW THIS DPA APPLIES TO CONTRACTOR AND ITS AFFILIATES?

If the Contractor entity signing this DPA is the Contractor under the Agreement, this DPA is an addendum to and forms part of the Agreement. If the Contractor Affiliate is a contractual party to this DPA by effect of Section 8 below, this DPA is binding onto VTEX and this Contractor Affiliate. In such a case, references to "VTEX" in this DPA shall mean the VTEX entity that is party to the Agreement.
If the Contractor entity signing this DPA has executed an Order Form - Commercial Proposal with VTEX or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form - Commercial Proposal and applicable renewal Order Form - Commercial Proposals, and references to "VTEX" in this DPA shall mean the VTEX entity that is party to such Order Form - Commercial Proposal.

1. DEFINITIONS

For the purposes of this DPA, any terms in capitalised letters that are not defined below or otherwise in this DPA or in the applicable Data Protections Laws, will have the meanings given to them in the Agreement.
"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common

control with the subject entity. “Control” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
“**Authorised Users**” means any person authorised by VTEX in writing to have control over VTEX Platform environment and any person who is given access by Contractor to VTEX Platform environment in accordance with the requirements set out in the Agreement.
“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data. For the purposes of this DPA, the Controller is the Contractor (as defined in the Agreement) and/or any Contractor Affiliate.
“**Contractor Affiliate**” means any of Contractor's Affiliate(s) (a) (i) that are subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom or any other applicable Data Protection Laws, and (ii) permitted to use the Services pursuant to the Agreement between Contractor and VTEX, but have not signed their own Order Form - Commercial Proposal and are not a “Contractor” as defined under the Agreement, (b) if and to the extent VTEX processes Personal Data for which such Affiliate(s) qualify as the Controller.
“**Contractor**” means the entity that is the contracting party to the Agreement and that is signing this DPA, on behalf of itself and on behalf of any and all Contractor Affiliates, as the case may be.
“**Contractor Data**” means all data and information submitted by Authorised Users to the Services and includes message text, files, comments and links, excluded Non-VTEX Products. Contractor Data does not include any Personal Data relating to Authorised Users received for the purposes of authorising access to the Services, or the representatives of the Contractor or Contractor Affiliates in connection with execution and administration of the Agreement or this DPA, which Personal Data VTEX processes as a controller.
“**Data Protection Laws**” means (i) the GDPR, (ii) any legislation in force from time to time in any Member State of the European Union or the European Economic Area, Switzerland and the United Kingdom relating to privacy or the processing of personal data; (iii) any legislation in force from time to time in any other covered jurisdiction; and (iv) any guidance or statutory codes of practice issued or adopted by any Supervisory Authority or other applicable data protection authority or a Data Protection Board in relation to such legislations, in any case as applicable to the Processing of Personal Data under the Agreement and as updated, amended, replaced or superseded from time to time.
“**Data Subject**” means the identified or identifiable natural person to whom the Personal Data relates.

“**EU Restricted Transfer”** means a transfer of Contractor Data including Personal Data by Contractor or any Contractor Affiliate to VTEX or any VTEX Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by European Data Protection Laws in the absence of the protection for the transferred Contractor Personal Data provided by the EU Standard Contractual Clauses.

“**EU Standard Contractual Clauses**” means the standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.
“**GDPR**” means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
“**UK Data Protection Laws”** means the GDPR as transposed into United Kingdom national law by operation 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 (“**UK GDPR**”), together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and other data protection or privacy legislation in force from time to time in the United Kingdom.
“**UK Restricted Transfer”** means a transfer of Contractor Personal Data by Contractor or any Contractor Affiliate to VTEX or any VTEX Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by UK Data Protection Laws in the absence of the protection for the transferred Customer Personal Data provided by the UK Standard Contractual Clauses.
“**UK Standard Contractual Clauses**” means the Standard Contractual Clauses (processors) set out in Decision 2010/87/EC and the Standard Contractual Clauses (controller) set out in Decision 2004/915/EC, as amended or replaced from time to time, pursuant to Article 46 of the UK GDPR.

"**Personal Data**" means any Contractor Data that relates to an identified or identifiable natural person, to the extent that such information is protected as personal data under applicable Data Protection Laws.
"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"**Processor**" means the entity which Processes Personal Data on behalf of the Controller. For the purposes of this DPA, the Processor is VTEX.

"**VTEX**" means the VTEX entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES TO CONTRACTOR AND ITS AFFILIATES" above.
"**VTEX Group**" means VTEX and its Affiliates engaged in the Processing of Personal Data.
"**Sub-processor**" means any entity engaged by VTEX, including a member of the VTEX Group as a sub-processor, to Process Personal Data in connection with the Services.
"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to Article 51 the GDPR and any similar regulatory authority responsible for the enforcement of Data Protection Laws (including the UK Information Commissioner's Office).

2. PROCESSING OF PERSONAL DATA
2.1. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data in the context of performance of the Agreement, Contractor is the Controller, VTEX is the Processor and that VTEX will engage Sub-processors pursuant to the requirements set forth in Section 4 "Sub-processors" below. The parties agree that, to the extent VTEX and/or any VTEX Affiliate is acting as Controller in relation to Contractor's individual business contacts' Personal Data, and Contractor is acting as Controller in relation to VTEX's individual business contacts' Personal Data, each act as a separate and independent Controller from Contractor and/or Contractor Affiliates.
2.2. **Contractor's Processing of Personal Data**. Contractor shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of Data Protection Laws.
Contractor shall have sole responsibility for the accuracy, quality, and lawfulness of Personal Data and the means by which Contractor acquired the Personal Data provided to VTEX. Contractor warrants that it has all necessary rights and needed consents, when required, from Data Subjects to share the Personal Data with VTEX and for VTEX to process the Personal Data as contemplated in the Agreement and this DPA.
2.3. **VTEX's Processing of Personal Data**. As Contractor's Processor, VTEX and any person acting under its authority or that of a VTEX Affiliate, who has access to Personal Data, shall only Process Personal Data in accordance with Data Protection Laws (as applicable to Processors) and comply with all obligations applicable to Processors under such laws and shall:
(i) Process the Contractor Personal Data in accordance with the Agreement, including for the provision and maintenance of the Services and for the use of the Services by Authorised Users;
(ii) Processing resulting from the use of the Services by Authorised Users; and
(iii) Process the Contractor Personal Data in accordance with reasonable and documented instructions provided by Contractor (e.g., via email or support tickets) that are consistent with the terms of the Agreement;
(individually and collectively, the "**Purpose**")
(iv) Not process that Personal Data except on instructions from the Contractor, unless required to do so by UK, European Union or Member State law or any Data Protection Laws to which the relevant contracted Processor is subject, in which case VTEX or the relevant VTEX Affiliate shall inform Contractor or the relevant Contractor Affiliate of that legal obligation before such Processing, unless that law prohibits such information on important grounds of public interest. When processing Special Categories of Data as defined in Appendix 1 or native Categories of Data with processes that were customised by the Controller or its commissioned actors, VTEX's responsibility is limited to the storage of this data. This DPA and the Agreement are Contractor's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions

must be requested separately in writing to VTEX; and

(v) inform Contractor or relevant Contractor Affiliate if, in the VTEX or relevant VTEX Affiliate's opinion, instructions given by the Controller infringe Data Protection Laws.
2.4**. Details of the Processing**. The subject-matter of Processing of Personal Data by VTEX is described in the Purpose in Section 2.3. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Appendix 1 (Description of Processing Activities) to this DPA.

3. RIGHTS OF DATA SUBJECTS
3.1. **Data Subject Requests**. VTEX shall, to the extent legally permitted, promptly redirect a Data Subject Request to Contractor if VTEX receives any requests from a Data Subject to exercise their Data Subject rights under the Data Protection Laws in relation to Personal Data: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making, as well as any other additional rights granted by the relevant Data Protection Laws to certain Data Subjects, as applicable (each, a "**Data Subject Request**"). Taking into account the nature of the Processing, VTEX shall assist Contractor by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Contractor's obligation to respond to a Data Subject Request under applicable Data Protection Laws. In addition, to the extent Contractor, in its use of the Services, does not have the ability to address a Data Subject Request, VTEX shall, upon Contractor's instruction, provide commercially reasonable efforts to assist Contractor in responding to such Data Subject Request, to the extent VTEX is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Contractor shall be responsible for any costs arising from VTEX's provision of such assistance, including any fees associated with the provision of additional functionality(ies).

4. SUB-PROCESSORS
4.1. **Appointment of Sub-processors.** Contractor acknowledges and generally agrees that (a) VTEX's Affiliates may be retained as Sub-processors under this DPA and (b) VTEX and VTEX's Affiliates respectively may engage third-party Sub-processors, in connection with the provision of the Services. As a condition to permitting a Sub-processor to Process Personal Data, VTEX (or a VTEX Affiliate acting as Sub-processor) will enter into a written agreement with each Sub-processor, containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA and, as the case may be, in EU Standard Contractual Clauses (Module 3) or in UK Standard Contractual Clauses (Processors), to the extent applicable to the nature of the Services provided and the Personal Data processed by such Sub-processor.
4.2. **List of Current Sub-processors and Notification of New Sub-processors**. A current list of Sub- processors engaged by VTEX for the provision of the Services, including the identities of those Sub-processors and their country of location, is available in APPENDIX 1 to this DPA. Such list may be updated and will remain accessible via https://vtex.com/us-en/privacy-and-agreements/subprocessors/ ("**Sub-processor List**"). VTEX shall maintain an updated List of the Sub-processors before authorised to Process Personal Data in connection with the provision of the applicable Services.

5. SECURITY
5.1. **Controls for the Protection of Personal Data**. VTEX shall maintain appropriate technical and organisational measures for protection of the security, confidentiality and integrity of Personal Data in the context of the provision of the Services. VTEX's current measures are set forth in Appendix 2 to this DPA and may change from time to time to maintain compliance with this DPA and/or applicable Data Protection Laws. VTEX regularly monitors compliance with these measures. VTEX will not materially decrease the overall security of the Services during a subscription term.
5.2. **Third-Party Certifications and Audits**. VTEX has obtained the third-party certifications and audits set forth in Appendix 2. Upon Contractor's request, and subject to the confidentiality obligations set forth in the Agreement, VTEX shall make available to Contractor (or Contractor's independent, third-party auditor) information regarding the VTEX Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Appendix 2. Contractor may contact VTEX to request an on-site audit of VTEX's procedures relevant to the protection of

Personal Data in the context of the Services, but only to the extent required under Data Protection Laws. Contractor shall reimburse VTEX for any time expended for any such on-site audit at the VTEX Group's then-current rates, which shall be made available to Contractor upon request. Before the commencement of any such on-site audit, Contractor and VTEX shall mutually agree upon the scope, timing, and duration of the audit and any measures to protect the security of third party personal data or VTEX confidential information, in addition to the reimbursement rate for which Contractor shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by VTEX. Contractor shall promptly notify VTEX with information regarding any non-compliance discovered during the course of an audit, and VTEX shall use commercially reasonable efforts to address any confirmed non-compliance.

6. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

VTEX maintains security incident management policies and procedures specified in the Appendix 2.
VTEX shall notify Contractor without undue delay of any Personal Data Breach of which VTEX becomes aware as required by Data Protection Laws or the Standard Contractual Clauses, as applicable. VTEX shall provide commercially reasonable cooperation and assistance in identifying the cause of such Personal Data Breach and take commercially reasonable steps to assist in the investigation, containment and remediation, including measures to mitigate its adverse effects, to the extent the remediation is within VTEX's control. VTEX shall document any Personal Data Breach, comprising the facts relating to the Personal Data Breach, its effects and the remedial action implemented by VTEX, as long as the remediation is within VTEX's control.

7. RETURN AND DELETION OF PERSONAL DATA

VTEX shall, upon Contractor's request no later than 30 days prior the termination of the Agreement and subject to the limitations described in the Agreement and the Appendix 2, provide the means for the Contractor to extract a complete copy of all Contractor Personal Data in VTEX's possession or, in the absence of any instructions from the Contractor, securely destroy such Personal Data, and demonstrate through a written certification to Contractor that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data or requires storage thereof, in which case VTEX warrants that it will continue to ensure compliance with this DPA and will only process the necessary data to the extent and for as long as required under that applicable law. Contractor acknowledges that VTEX may comply with the above obligation by providing the interfaces necessary to the Contractor to retrieve the Personal Data by its own means. For clarification, data that is not available for self-service retrieval may incur additional charge(s) to be supported by Contractor.

8. CONTRACTOR AFFILIATES

8.1. **Contractual Relationship**. The parties acknowledge and agree that, by executing the DPA, Contractor enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of the Contractor Affiliates, thereby establishing a separate DPA between VTEX and each such Contractor Affiliate subject to the provisions of the Agreement and Section 8 of this DPA. The Contractor warrants that it has the power and authority to enter into the DPA on behalf of itself and, as applicable, in the name and on behalf of the Contractor Affiliates. Each Contractor Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Contractor Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Contractor Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions of the Agreement and this DPA by a Contractor Affiliate shall be deemed a violation by Contractor.
8.2. **Communication.** The Contractor that is the contracting party to the Agreement shall remain responsible for coordinating all communication with VTEX under the Agreement and this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates.
8.3. **Rights of Contractor Affiliates**. If a Contractor Affiliate becomes a party to the DPA with VTEX, it shall, to the extent required under Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, subject to the following:
8.3.1. Except where Data Protection Laws require the Contractor Affiliate to exercise a right or seek any remedy under this DPA against VTEX directly by itself, the parties agree that (i) solely the Contractor that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Contractor Affiliate, and (ii) the Contractor that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Contractor

Affiliate individually but in a combined manner for all of its Contractor Affiliates together (as set forth, for example, in Section 8.3.2, below).
8.3.2. The parties agree that the Contractor that is the contracting party to the Agreement shall, if carrying out an on-site audit of the VTEX procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on VTEX by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Contractor Affiliates in one single audit.

9. LIMITATION OF LIABILITY
Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Contractor Affiliates and VTEX, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.
For the avoidance of doubt, VTEX's and its Affiliates' total liability for all claims from the Contractor and all of Contractor Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Contractor and all Contractor Affiliates, and, in particular, shall not be understood to apply individually and severally to Contractor and/or to any Contractor Affiliate that is a contractual party to any such DPA.

10. EUROPEAN SPECIFIC PROVISIONS
10.1. **Data Protection Laws**. VTEX Processes Personal Data in accordance with the Data Protection Laws to the extent directly applicable to VTEX's provisioning of the Services.
10.1.1. **Data Protection Impact Assessment**. Upon Contractor's request, VTEX shall provide Contractor with reasonable cooperation and assistance needed to fulfil Contractor's obligation under the Data Protection Laws to carry out a data protection impact assessment related to Contractor's use of the Services, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons and to the extent Contractor does not otherwise have access to the relevant information, and to such information is available to VTEX. VTEX shall provide reasonable assistance to the Contractor to consult the Supervisory Authority, prior to the Processing, to the extent required under the Data Protection Laws.
10.1.2. VTEX will notify the Contractor if it believes an instruction infringes the GDPR or other European Union or Member State Data Protection Laws.
10.1.3. **Restricted Transfers**. The Parties acknowledge that in providing the Services, VTEX will transfer Personal Data to recipients (including VTEX partners and Sub-processors) that may be located in countries outside the EEA. Such countries may not be deemed to offer an adequate level of data protection, as defined by the Data Protection Laws. Consequently, such transfers of Personal Data will be protected by appropriate safeguards mandated by the Data Protection Laws, including as the case may be the EU Standard Contractual Clauses, UK Standard Contractual Clauses or any additional safeguards as required by Data Protection Laws (each, a "**Restricted Transfer**").
In respect of any Restricted Transfer, the parties agree to the following:
10.1.3.1 In respect of any **EU Restricted Transfer**, Contractor and each Contractor Affiliate (each as "data exporter") and VTEX and each VTEX Affiliate (each as "data importer") with effect from the commencement of the relevant transfer hereby enter into the Module 2 – Controller to Processor of the EU Standard Contractual Clauses, the processing operations are deemed to be those described in Appendix 1 to this DPA. Appendix 2 to this DPA include the Technical and Organisational Measures applicable to the data transferred in the context of the processing activities carried out under this DPA.
10.1.3.2 In respect of any **UK Restricted Transfer**, Contractor acting on its own behalf and as agent for each Contractor Affiliate (each as "data exporter") and VTEX acting on its own behalf and as agent for each VTEX Affiliate or contracted Processor (each as "data importer") with effect from the commencement of the relevant transfer hereby enter into the UK Standard Contractual Clauses (processors) set out in Decision 2010/87/EC, the processing operations are deemed to be those described in Appendix 1 to this DPA. Appendix 2 to this DPA include the Technical and Organisational Measures applicable to the data transferred in the context of the processing activities carried out under this DPA. If at any time the UK Government approves UK-specific standard contractual clauses (processors) for use under the UK Data Protection Laws, the provisions of clause 10.1.3.2 shall be construed as implementing such UK-specific standard contractual clauses (processors) in respect of UK Restricted Transfers. In that respect, the governing law of the UK-specific standard contractual

clauses shall be English law and the supervisory authority be the Information Commissioner's Office.
10.1.3.3 The EU Standard Contractual Clauses made under clause 10.1.3.1 and the UK Standard Contractual Clauses made under clause 10.1.3.2 of this DPA, as applicable, come into effect on the later of:
- the Data Exporter becoming a Party to this DPA;
- the Data Importer becoming a Party to this DPA; and
- the commencement of the EU Restricted Transfer or UK Restricted transfer (as applicable) to which the EU Standard Contractual Clauses or the UK Standard Contractual Clauses relate.
10.1.3.4 If, at any time, a Supervisory Authority or a court with competent jurisdiction over a party mandates that transfers from Controllers in the EEA or the UK to Processors established outside the EEA or the UK must be subject to specific additional safeguards (including but not limited to specific technical and organisational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Contractor Personal Data is conducted with the benefit of such additional safeguards.
10.1.4. **Onward transfers to Sub-processors.** The Parties acknowledge that, in providing the Services, VTEX will carry out Restricted Transfers to Sub-processors, in accordance with clause 10.1.3 of this DPA.
10.1.5. **Confidentially**. VTEX will ensure that persons authorised to Process Personal Data are subject to an appropriate contractual or statutory obligation of confidentiality.

11. LEGAL EFFECT
This DPA shall only become legally binding between Contractor and VTEX when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed. If Contractor has previously executed a data processing addendum with VTEX, this DPA supersedes and replaces such prior data processing addendum.

12. GOVERNING LAW
As established in the Clause "Governing Law" in the Master Services Agreement.
As an exception to the foregoing, in respect of UK Restricted Transfers only, "governing law" shall be the laws of England.

13. DATA PROCESSING ACTIVITIES
The subject matter of the Processing of the Contractor Personal Data; the duration of the Processing; the nature and purpose of the Processing of the Contractor Personal Data; and the details of the obligations and rights of the Contractor and VTEX are as set out in Appendix 1B of this DPA.

Location, date and signatures on the Order Form - Commercial Proposal

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the DPA Effective Date first set out above.

APPENDIX 1 - DESCRIPTION OF THE PROCESSING

1A. LIST OF PARTIES AND SUBPROCESSORS

We made available all parties through our website:
https://vtex.com/us-en/privacy-and-agreements/subprocessors/

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

1. **Controller to Processor**

    a. **Data exporter: VTEX CUSTOMER - IT MEANS THE CLIENT/CONTRACTING PARTY IDENTIFIED IN THE MASTER SERVICES AGREEMENT.**
    Role (controller/processor): Controller

    b. **Data importer: VTEX ENTITY IDENTIFIED IN THE MASTER SERVICES AGREEMENT**
    Role (controller/processor): Processor

    c. **Data importer: VTEX BRAZIL**
    Name: VTEX Brasil Tecnologia para E-commerce LTDA
    Address: Avenida Brigadeiro Faria Lima, nº 4.440, 10º andar, Vila Olímpia, CEP 04538-132, inscrita no CNPJ/MF sob o n. 05.314.972/0001-74
    Role (controller/processor): Subprocessor

    d. **Data importer (or exporter, in case Ireland applies): AWS**
    Name: Amazon Web Services Inc.
    Address: United States / work in progress to launch storage in AWS Ireland by 2023, depending on the complexity of functionalities.
    Role (controller/processor): Subprocessor

1B. DESCRIPTION OF TRANSFER

Subject matter and duration of the processing of the Personal Data.
The subject matter of the Processing of the Contractor Personal Data are as set out in the Agreement and this DPA. Processing operations are carried out in the context of the performance of the Agreement for the provision and management of the Services by VTEX to the Contractor.
The duration of the Processing is aligned to that of the Agreement.

Nature of the processing, purpose(s) of the data transfer and further processing

The Personal Data transferred will be processed for the purposes of the Services to be provided under the Agreement and any Order Form - Commercial Proposal and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain, and update the Services provided to the Contractor;
- to provide Contractor maintenance and technical support ; and
- disclosures in accordance with the Agreement, as compelled by law.

There is no further processing other than transfers to subprocessors.
The categories of Data Subject to whom the Contractor Personal Data relates

The categories of Data Subject may include some or all of the following:

- Contractor's personnel;
- Contractor's end-users (clients)

The types of Personal Data to be processed: IP; navigation Information such as cookies; cart information; order information; email; phone number; address; ID number, gift card history; name; order history; navigational information; unused cart; conversations; sessions passwords; generated tokens; sessions.

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

Data Exporters may submit special categories of Personal Data to the Data Importer as the case may be, through the Services, the extent of which is determined and controlled by the Data Exporter in compliance with applicable Data Protection Laws.

The obligations and rights of the Contractor and VTEX.
The details of the obligations and rights of the Contractor and VTEX are as set out in the Agreement and this DPA.

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

Data is transferred on a continuous basis for the purposes of the Services to be provided under the Agreement and any Order Form - Commercial Proposal.

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

To be mutually agreed between Contractor and VTEX, in accordance with applicable laws governing privacy, e-commerce transactions and tax laws.

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

VTEX hires Amazon Web Services Inc. and Microsoft Inc. (Azure) as Cloud Service Providers for hosting purposes for the duration of the Master Services Agreement executed by and between VTEX and Contractor. Please see Appendix 1.

COMPETENT SUPERVISORY AUTHORITY

Defined by the Contractor.

APPENDIX 2

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

The Data Importer has implemented and will maintain appropriate technical and organisational measures to protect the personal data against misuse and accidental loss or destruction as set forth in VTEX Privacy and Security Policies.
The Data Importer's current technical and organisational measures are set forth below.
As mentioned above, below is a non-exhaustive list of points that are currently implemented in VTEX with a focus on data protection and security considering the triad of: IT, Security and Privacy.

1. Awareness and Training
    a. The company has training cycles for different levels of employees with a focus on privacy and security. VTEX will also have training focused on good practices in secure development.
2. Password protection
    a. VTEX currently saves passwords in one way: HashVector(Main Algorithm used here is PBKDF2 with SHA256).
3. Anti-virus Policy
    a. The IT team has a policy of keeping all of its staff computers with antivirus.
4. Data classification
    a. VTEX has an information classification policy to understand what type of protection each type of data needs.
5. Vulnerability management
    a. VTEX performs regular threat and vulnerability reviews of the platform and operation processes. Risk identification triggers the improvement of our monitoring and notification systems to handle their eventual materialisation, be it by notifying personnel who are able to deal with it or by triggering automated actions that can mitigate or eliminate them. In point 15 of the appendix we bring the functioning of our pentests in detail.
6. Certifications
    a. As defined by industry standards, company certifications will typically cover a period from January to December, December being the month to renew the certification for that current year. Hence, when we speak of the current certifications we have, we are referring to those we have maintained until the last possible period. The certifications VTEX has maintained until the last applicable period, therefore, are:
        i. SOC 1 - Type 2: A report covering internal controls over financial reporting systems;
        ii. SOC 2 - Type 2: A report covering Security, Availability, Integrity, Confidentiality, and Privacy;
        iii. SOC 3 - A public report of Security, Availability, Integrity, Confidentiality and Privacy Controls;
        iv. PCI - A validation of controls around cardholder data to reduce credit card fraud.
        v. All of these certifications are available under the Compliance section on the VTEX Trust Hub (https://vtex.com/us-en/trust/)
7. VTEX measures to ensure the security of the data
    a. The data in transit is always encrypted, in addition to that VTEX have in-house solutions for building application security, and also carry out test cycles with third-party companies in order to improve our solutions in addition to the use of backup policies and evaluation of possible failures and incident reviews. Finally, external audits ensure that most of these flows: Data anonymization, secure processing, among

others, are respected and carried out.

8. How we address Data Backup and Redundancy
    a. Most of the data handled by VTEX is stored on AWS services using managed services such as S3, RDS and DynamoDB. All of those services provide AWS managed backup infrastructure that is used by VTEX. The AWS platform is a reference in the cloud computing industry and holds important certifications such as: ISO 27001, PCI DSS, CSA, NIST and many others. (To see a list of detailed certifications, access: https://aws.amazon.com/en/compliance/programs/)
9. Disaster Recovery and Incident Recovery
    a. VTEX's Disaster and Incident Recovery Plan consists of internal policies and procedures that VTEX will follow in case of service disruption. This could happen because of a natural disaster, or as a result of technological failure or human factors. The goal is to restore the affected business processes as quickly as possible, whether by bringing the disrupted services back online or by switching to a contingency system.
    b. The scope of this plan is VTEX Cloud Commerce Platform, including: (i) all services that constitute the solution; (ii) all business processes that support it or its operation; (iii) all business processes that support VTEX's clients who depend on VTEX Cloud Commerce Platform;
    c. VTEX's Disaster and Incident Recovery Plan is fully supported and implemented by automated processes that are triggered based on also automated monitoring and notification tools.
    d. Recovery Time Objective (RTO): is the maximum amount of time that should be allowed to elapse before normal services are resumed. Service downtime may be related to application disruption, data corruption or data loss, data server failure, or AWS Availability Zone or Region disruption. VTEX's Disaster and Incident Recovery Plan is tested at least annually, in order to see that it will be effective at any moment it is needed.
    e. External stakeholders are notified through the status page (https://status.vtex.com): the status page is publicly available to anyone interested in seeing VTEX True Cloud CommerceTM platform current health status. It is also used as a notification tool for planned maintenance, which is not in the scope of the DRP.
10. Private Data Encryption
    a. As of today, and following our commitment to compliance with the GDPR, VTEX guarantees encryption according to what the privacy and compliance regulations surrounding PII require. For example, our Payments Product is PCI compliant and implements data encryption and key rotation according to the PCI DSS standards. On top of this, VTEX has ongoing engineering projects to implement encryption and isolation of PII data as well as to implement audit logging in a multitude of applications on top of those of ours that already offer it.
11. Data Storage at VTEX
    a. VTEX's hosting provider is AWS, the world's leading provider of cloud computing services, and the data is stored in the AWS region of Northern Virginia, United States. There is work in progress to launch storage in AWS Ireland by 2023, depending on the complexity of functionalities. One of the key pillars of AWS is "Security is Job Zero", a statement that proves that information security is placed before anything else in AWS with which VTEX strongly identifies.
12. Data Transmission
    a. All incoming traffic into VTEX's network is protected using TLS 1.2 technology over http.
13. Customer and Network Segregation
    a. Production network is completely isolated from external networks. VTEX employees responsible for production environments operation may need eventual VPN connection to access the production network.

14. Physical Security and Environmental Protection
    a. The physical assets utilised by VTEX are provided by AWS as part of the service provided by them.
15. Pentest policies

    Due to the nature of VTEX's business, we are building a policy of performing quarterly penetration tests, currently the tests take place annually. In addition, several clients independently evaluate our platform, so we are always audited both externally and internally.
16. Controls for sub processors

    VTEX has a sub processor analysis questionnaire that includes some security questions to analyse the potential risks of each relationship. The methods used to assess the security of third parties are selected by considering the type and severity of risks in these relationships, the adequacy and relevance of the details that can be obtained about security processes and controls. More specifically, AWS, listed as a subprocessor in Appendix 1, holds security and privacy certifications ISO 27017:2015 and ISO 27018:2014, which are subsets based on ISO 27001:2013, the most comprehensive security standard.

APPENDIX 3

– EU STANDARD CONTRACTUAL CLAUSES CONTROLLER TO PROCESSOR (MODULE 2)

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 Appendix 1 (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 Appendix 1. (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 Appendix 1

(d) The Appendix to these Clauses containing the Appendix 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);

(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 Appendix 1.

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 Appendix 1.

(b) Once it has completed the Appendix and signed Appendix 1, 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 Appendix 1.

(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 Appendix 1. , 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 Appendix 2 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Appendix 1 After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Appendix 2. 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 Appendix 1.

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 benefiting 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 noncompliance. 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 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

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 Appendix 2 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 Appendix 1, shall act as a competent supervisory authority.

(b) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Appendix 1, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practises affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practises 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 practises 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 practises 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 practises 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 set out in the

Master Services Agreement.

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 defined in the Master Services Agreement.

(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.

APPENDIX 4
– UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Table 2: Selected SCCs, Modules and Selected Clauses

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

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	Controller to Processor	Yes	Yes	General Authorisation	15 days	No

Table 3: Appendix Information

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

Annex 1A: List of Parties:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only): listed in Annex 1A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: □ Importer □ Exporter X neither Party

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this 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 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 Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this 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:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
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.
Approved Addendum	The template 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.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
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.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This 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 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 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 Addendum, UK Data Protection Laws applies.

7. If the meaning of this 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, re-enacted and/or replaced after this 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 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 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 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. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 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. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

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.

Amendments to this 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 Addendum including the Appendix Information. This 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 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 Addendum, but any changes must be made in accordance with its terms.

***

1. ments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this 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. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 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. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

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.

Amendments to this Addendum

2. 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.

3. 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.

4. 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 Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

5. 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 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.

6. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

***