MASTER DATA PROTECTION AGREEMENT

This Master Data Processing Addendum ("MDPA") is incorporated by reference into the agreement governing the use of Vertice's services ("Agreement") entered by and between you, the Customer (as defined in the Agreement) ("Customer"), and the Vertice entity set forth in the Agreement ("Vertice") to reflect the parties' agreement with regard to the Processing of Personal Data by Vertice solely on behalf of the Customer. Both parties shall be referred to as the "Parties" and each, a "Party".

Unless otherwise specified in this MDPA, the terms of the Agreement shall continue in full force and effect. All capitalised terms not defined in this MDPA shall have the meanings set forth in the Agreement. Any privacy or data protection related clauses or agreement previously entered into by Vertice and Customer, shall be superseded and replaced with this MDPA.

This agreement was last updated on November 7th, 2022. It is effective between Customer and Vertice as of the date of Customer's accepting this Agreement (the "Effective Date").

The parties agree as follows:

1. **Definitions**
   - 1.1. "**Affiliates**" means companies within the Vertice group that may Process Customer Personal Data in order to provide the Services.
   - 1.2. "**Agreement**" means the written or electronic agreement between Customer and Vertice for the provision of the Services to Customer.
   - 1.3. "**APEC**" means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information.
   - 1.4. "**APEC Member Economy**" means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.
   - 1.5. "**Approved Jurisdiction**" means a member state of the EEA, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
   - 1.6. "**Controller**" means an entity that determines the purposes and means of the processing of Personal Data.
   - 1.7. "**Data Breach**" means a breach of Security Measures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
   - 1.8. "**Data Protection Laws**" means all mandatory applicable laws that apply to the Processing of Personal Data under the Agreement.
   - 1.9. "**Data Subject**" means the individual to whom Personal Data relates.
   - 1.10. "**EEA**" means those countries that are members of European Free Trade Association ("EFTA"), and the then-current, post-accession member states of the European Union.
   - 1.11. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council 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).
   - 1.12. "**Personal Data**" means any information about, or related to, an identifiable individual Processed on behalf of the Customer. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.
   - 1.13. "**Processing**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organisation, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "**Processes**" and "**Process**" shall be construed accordingly.
   - 1.14. "**Processor**" means an entity that processes Personal Data on behalf of a Controller.
   - 1.15. "**Representatives**" means either Party including its Affiliates' officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.
   - 1.16. "**Security Measures**" means the technical and organisational measures designed to protect the Personal Data as set forth in Attachment A.
   - 1.17. "**Special Categories of Personal Data**" means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, certain financial information when identified as such by mandatory applicable law, precise geolocation over time and data related to offenses or criminal convictions.
   - 1.18. "**Services**" means the services purchased by Customer from Vertice under the Agreement.
   - 1.19. "**Standard Contractual Clauses**" means the agreement set forth in Attachment B as approved by the European Commission for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection and any subsequent changes approved by the European Commission with an official decision.
   - 1.20. "**Subprocessor**" means another Processor engaged by Vertice to carry out Processing of Customer's Personal Data.

2. **Obligations of the Parties**
   - 2.1. The Parties agree that, for this MDPA, Customer shall be the Controller and Vertice shall be the Processor.
   - 2.2. Customer shall:
     - 2.2.1. use the Services in compliance with Data Protection Laws;

2.2.2. ensure all instructions given by it to Vertice in respect of the Processing of Personal Data are at all times in accordance with Data Protection Laws;

2.2.3. ensure all Personal Data provided to Vertice has been collected in accordance with Data Protection Laws and that Customer has all authorizations and/or consents necessary to provide such Personal Data to Vertice; and

2.2.4. keep the amount of Personal Data provided to Vertice to the minimum necessary for the provision of the Services.

2.3. Vertice shall:

2.3.1. only Process the Personal Data in accordance with Customer's documented instructions, Annex 1 to the Standard Contractual Clauses (where applicable) and this MDPA;

2.3.2. promptly notify Customer if Vertice reasonably believes that Customer's instructions are inconsistent with Data Protection Laws;

2.3.3. ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Vertice to keep the Personal Data confidential;

2.3.4. appoint data protection lead(s) and, upon request, provide the contact details of the appointed person(s);

2.3.5. assist Customer as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Vertice's Processing of Personal Data;

2.3.6. if required by Data Protection Laws, court order, subpoena, or other legal or judicial process to Process Personal Data other than in accordance with Customer's instructions, notify Customer without undue delay of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such notification, in particular on important grounds of public interest);

2.3.7. only Process Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;

2.3.8. where applicable, act as a subprocessor of such Personal Data;

2.3.9. maintain records of the Processing of any Personal Data received from Customer under the Agreement;

2.3.10. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by the Parties in a separate agreement;

2.3.11. provide such assistance as Customer reasonably requires (either on its own behalf or on behalf of its customers), and Vertice or a Representative is able to provide, in order to meet any applicable filing, approval or similar requirements in relation to Data Protection Laws;

2.3.12. provide such information and assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to Vertice) to enable compliance by Customer with its obligations under Data Protection Laws with respect to:

2.3.12.1. security of Processing;

2.3.12.2. data protection impact assessments (as such term is defined by the GDPR);

2.3.12.3. prior consultation with a supervisory authority regarding high-risk Processing; and

2.3.12.4. notifications to the applicable supervisory authority and/or communications to Data Subjects by Customer in response to any Data Breach;

2.3.13. on termination of the MDPA for whatever reason, cease to Process Personal Data, and upon Customer's written request and without undue delay, (i) return, or make available for return, Personal Data in its possession or control, or (ii) securely delete or permanently render unreadable or inaccessible existing copies of the Personal Data; unless continued retention and Processing is required or is permitted by Data Protection Laws and/or mandatory applicable law. At Customer's request, Vertice shall give Customer confirmation in writing that it has fully complied with this Section 2.3(m) or provide a justification as to why such compliance is not feasible.

3. Transfers of Personal Data

3.1. Transfers of Personal Data from EEA or Switzerland to third countries. Where Vertice Processes Personal Data from the EEA or Switzerland on behalf of Customer, in a country which is not an Approved Jurisdiction, Vertice shall perform such Processing in accordance with the Standard Contractual Clauses set forth in Attachment B to this MDPA and/or in accordance with Articles 44 to 49 of the GDPR.

3.2. Transfers of Personal Data from the UK to third countries. Where Vertice Processes Personal Data from the UK in a third country, such Processing shall be performed in accordance with Attachment B, as amended by the UK Addendum to the EU Commission Standard Contractual Clauses included in Attachment C (the "Addendum"). Any further changes to this Addendum approved with an official decision by the Information Commissioner's Office will be incorporated by reference.

3.3. Transfers of Personal Data from jurisdictions other than the EEA, Switzerland or UK to third countries. For jurisdictions other than the EEA or Switzerland, Vertice shall not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under Data Protection Laws. Where Vertice Processes Personal Data from an APEC Member Economy on behalf of Customer, Vertice shall perform such Processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("**CBPRs**") (see www.cbprs.org) to the extent the requirements are applicable to Vertice's Processing of the Personal Data. If Vertice is unable to provide the same level of protection as required by the CBPRs, Vertice shall promptly notify Customer and cease Processing. In such event, Customer may terminate the Agreement with respect only to those Services for which Vertice is unable to provide the same level of protection as required by the CBPRs by written notice within 30 days.

4. Subprocessing

4.1. Vertice shall not subcontract its obligations under this MDPA to new Subprocessors, in whole or in part, without providing Customer with notice and an opportunity to object. If Customer objects to the proposed subcontracting on reasonable grounds related to the protection of

the Personal Data and the Parties cannot resolve the objection, the Customer may terminate the applicable part of the Agreement with respect only to those Services which cannot be provided by Vertice without the use of the objected to Subprocessors by giving written notice to Vertice.

4.2. Where Vertice appoints a Subprocessor, Vertice will execute a written agreement with the Subprocessor(s) containing terms at least as protective as this MDPA.

4.3. Vertice shall be liable for the acts or omissions of Subprocessors to the same extent it is liable for its own actions or omissions under this MDPA.

4.4. For the purposes of Clause 9 of the Standard Contractual Clauses, Customer provides a general consent to Vertice to engage Subprocessors. Such consent is conditional on Vertice's compliance with Section 4 of this MDPA.

5. Rights of Data Subjects

5.1. Data Subject requests. Vertice shall, to the extent legally permitted, promptly redirect the Data Subjects to send their requests to the Customer or notify Customer if it receives a request from a Data Subject for access to, rectification, portability, objection, restriction or erasure of such Data Subject's Personal Data. Unless required by Data Protection Laws, Vertice shall not respond to any such Data Subject request without Customer's prior written consent except to redirect the Data Subject to the Customer. Vertice shall provide such information and cooperation and take such action as the Customer reasonably requests in relation to a Data Subject request.

6. Security

6.1. Controls for the Protection of Personal Data. Vertice shall implement and maintain appropriate technical and organisational measures designed to protect the Personal Data as set forth in the Security Measures. Vertice regularly monitors compliance with these Security Measures.

7. Audit

7.1. Vertice shall make available to the Customer such information as is reasonably necessary to demonstrate Vertice's compliance with the obligations of this MDPA in accordance with the terms of the Security Measures.

7.2. Vertice shall allow for and contribute to audits, including on-site inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by Vertice and Subprocessors. Any audit must be conducted during regular business hours and may not unreasonably interfere with Vertice's business activities.

8. Notification and Communication

8.1. Notification. Vertice shall notify Customer at the email address provided by Customer within 48 hours of confirmation of a Data Breach relating to Customer's Personal Data. Vertice shall provide all such timely information and cooperation as Customer may reasonably require in order for Customer to fulfil its Data Breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. Vertice shall further take such measures and actions as it considers necessary or appropriate to remedy or mitigate the effects of the Data Breach and shall keep Customer informed in connection with the Data Breach.

8.2. Information Security Communication. Except as required by mandatory applicable law, Vertice agrees that it will not inform any third party of a Data Breach referencing or identifying the Customer, without Customer's prior written consent. Vertice shall reasonably cooperate with Customer and law enforcement authorities concerning a Data Breach. Vertice shall retain, for an appropriate period of time, all information and data within its possession or control that is directly related to any Data Breach. If disclosure of the Data Breach referencing or identifying the Customer is required by mandatory applicable law, Vertice will work with Customer regarding the timing, content, and recipients of such disclosure.

8.3. Post-incident. Vertice shall reasonably cooperate with Customer in any post-incident investigation, remediation, and communication efforts.

8.4. Complaints or notices related to Personal Data. If Vertice receives any official complaint, notice, or communication that relates to its Processing of Personal Data or either Party's compliance with Data Protection Laws in connection with Personal Data, to the extent legally permitted, Vertice shall promptly notify Customer and, to the extent applicable, Vertice shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Vertice's provision of assistance in relation to any official complaint, notice, or communication that relates to Customer's compliance with Data Protection Laws.

9. General

9.1. Except for any liability which cannot be limited or excluded under mandatory applicable law, the aggregate liability of Vertice for all Data Breaches and any breach of this MDPA (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) shall not exceed US$100,000.

9.2. Where a Data Breach and/or breach of this MDPA is also a breach of any confidentiality or non-disclosure obligations in the Agreement, the liability cap in Section 9.1 will apply.

9.3. Nothing in this MDPA is intended to limit the Parties' direct liability towards data subjects or applicable supervisory data protection authorities which cannot be limited under mandatory applicable law.

9.4. No one other than a Party to this MDPA, their successors and permitted assignees shall have any right to enforce any of its terms.

9.5. This MDPA will become effective on the Effective Date and remain in force for the term of Agreement.

9.6. In the event of a conflict, the following order of precedence will apply:

(a) the Standard Contractual Clauses (as set out in Attachment B);
(b) this MDPA; and
(c) the Agreement (as set out in Annex I); and
(d) where applicable, any other agreement entered into between the Parties related to the Services.

9.7. Amendments to this MDPA must be mutually agreed upon by the Parties in writing. For the avoidance of doubt, where data transfers are made pursuant to the Standard Contractual Clauses, amendments shall be strictly limited to Annexes 1, 2 and 3 to Attachment B.

Attachment A
Security Measures

1. **Scope**
   1.1. This Attachment describes the technical and organisational security measures that shall be implemented by Vertice to secure Personal Data and Customer Content (collectively, "Data") prior to any processing under the Agreement.

2. **General Security Practices**
   2.1. Vertice has implemented and shall maintain appropriate technical and organisational measures designed to protect Data against accidental loss, destruction or alteration, unauthorised disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this Attachment for its Representatives, facilities, and equipment at Vertice's locations involved in Vertice's performance of its obligations under the Agreement.

3. **General Compliance**
   3.1. **Compliance**. Vertice shall document and implement processes to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes shall be designed to provide appropriate security to protect Data given the risk posed by the nature of the Data processed by Vertice. Vertice shall implement and operate information security in accordance with Vertice's own policies, which shall be no less strict than the information security requirements set forth in this document.
   3.2. **Protection of logs and records**. Vertice shall implement appropriate procedures designed to protect logs and records from loss, destruction, falsification, unauthorised access, and unauthorised release, in accordance with legislative, regulatory, and contractual requirements.
   3.3. **Review of information security**. Vertice's approach to managing information security and its implementation shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.
   3.4. **Compliance with security policies and standards**. Vertice's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.
   3.5. **Technical compliance review**. Vertice shall regularly review information systems for compliance with Vertice's information security policies and standards.
   3.6. **Information Risk Management**. Vertice shall implement and utilise an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. Threat and vulnerability assessments must be reviewed periodically and prompt remediation actions taken where material weaknesses are found.
   3.7. **Processing of Sensitive Personal Data**. To the extent that Vertice processes Sensitive Personal Data and the security measures referred to in this document are deemed to provide insufficient protection, Customer may request that Vertice implement additional security measures.

4. **Technical and Organisational Measures for Security**
   4.1. Organisation of Information Security
      4.1.1. **Security Ownership**. Vertice shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organisation.
      4.1.2. **Security Roles and Responsibilities**. Vertice shall define and allocate information security responsibilities in accordance with Vertice's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.
      4.1.3. **Project Management**. Vertice shall address information security in project management to identify and appropriately address information security risks.
   4.2. Human Resources Security
      4.2.1. **General**. Vertice shall ensure that its personnel are subject to confidentiality obligations and shall provide adequate training about relevant privacy and security policies and procedures. Vertice shall further inform its personnel of possible consequences of breaching Vertice's security policies and procedures, which must include disciplinary action, including possible termination of employment for Vertice's employees and termination of contract or assignment for relevant external Representatives (e.g., contractors, agents, consultants etc.).
      4.2.2. **Training**. Representatives with access to Data shall receive appropriate, periodic (i.e., at least annual) education and training regarding privacy and security procedures to aid in the prevention of unauthorised use (or inadvertent disclosure) of Data and training regarding how to effectively respond to security incidents. Training shall be provided before Representatives are granted access to Data or begin providing Services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.
   4.3. Access Controls
      4.3.1. **Access**.
         4.3.1.1. **Limited Use**. Vertice will not (i) access the Customer's computer systems for any purpose other than as necessary to perform its obligations under the Agreement or as otherwise agreed to by the parties; or (ii) use any system access information or log-in credentials to gain unauthorised access to Data or Customer's systems, or to exceed the scope of any authorised access.

4.3.1.2. **Authorization**. Vertice shall restrict access to Data and systems at all times solely to those Representatives whose access is necessary.

4.3.1.3. **Suspension or Termination of Access Rights**. At Customer's reasonable request, Vertice shall promptly and without undue delay suspend or terminate the access rights to Data and systems for any Representatives reasonably suspected of breaching any of the provisions of this document; and Vertice shall remove access rights of all Vertice employees and relevant external parties upon suspension or termination of their employment or engagement.

4.3.2. **Access Policy**. Vertice shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Vertice shall maintain a record of security privileges of Representatives that have access to Data, networks, and network services. Vertice shall restrict the use of utility programs that might be capable of overriding system and application controls.

4.3.3. Access Authorization

4.3.3.1. Vertice shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to its systems and networks. Vertice shall use an enterprise access control system that requires revalidation of Representatives by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

4.3.3.2. Vertice shall maintain and update a record of its users authorised to access systems that contain Data and Vertice shall review such users' access rights at regular intervals.

4.3.3.3. For systems that process Data, Vertice shall revalidate (or where appropriate, deactivate) access of Representatives who change Vertice reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.

4.3.3.4. Vertice shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, to prevent the introduction of unauthorised functionality and to avoid unintentional changes.

4.3.4. **Network Design**. For systems that process Data, Vertice shall have controls to avoid Representatives assuming access rights that could be used to gain unauthorised access to Data.

4.3.5. **Least Privilege**. Vertice shall limit Representatives' access to Data to those Representatives who have an actual need to access such Data to perform their assigned duties.

4.3.6. Authentication

4.3.6.1. Vertice shall use industry standard practices including ISO/IEC 27002:2013 and NIST SP 800- 63B (Digital Identity Guidelines) to identify and authenticate users who attempt to access information systems.

4.3.6.2. Where authentication mechanisms are based on passwords, Vertice shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability) with at least 8 characters and containing the following four classes: upper case, lower case, numeral, special character.

4.3.6.3. Vertice shall maintain industry standard procedures to prevent de-activated or expired identifiers and log-in credentials from being granted to other individuals.

4.3.6.4. Vertice shall monitor repeated failed attempts to gain access to its information systems.

4.3.6.5. Vertice shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

4.3.6.6. Vertice shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

4.3.6.7. Vertice shall implement a multi-factor authentication solution to authenticate Representatives accessing its information systems.

4.4. Physical and Environmental Security

4.4.1. Physical Access to Facilities

4.4.1.1. Vertice shall limit access to facilities where systems that process Data are located to authorised individuals.

4.4.1.2. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

4.4.1.3. Facilities shall be monitored and access-controlled at all times (24x7).

4.4.1.4. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems processing Data. Vertice must register authorised individuals and require them to carry appropriate identification badges.

4.4.2. **Physical Access to Equipment**. Vertice equipment used to process Data shall be protected using industry standard processes to limit access to authorised Representatives.

4.4.3. **Protection from Disruptions**. Vertice shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

4.4.4. **Clear Desk**. Vertice shall have policies requiring a "clean desk/clear screen" designed to prevent inadvertent disclosure of Data.

4.5. Operations Security

4.5.1. **Operational Policy**. Vertice shall maintain written policies describing its security measures and the relevant procedures and

responsibilities of Representatives who have access to Data and to its systems and networks. Vertice shall communicate its policies and requirements to all Representatives involved in the processing of Data. Vertice shall implement the appropriate management structure and control designed to maintain compliance with such policies and with mandatory applicable law concerning the protection and processing of Data.

4.5.2. **Logging and Monitoring**. Vertice shall maintain logs of administrator and operator activity and data recovery events related to Data.

4.6. Communications Security and Data Transfer

4.6.1. **Networks**. Vertice shall, at a minimum, use the following controls to secure its corporate networks that process Data:

4.6.1.1. Network traffic shall pass through firewalls, which are monitored at all times. Vertice must implement intrusion detection systems and/or intrusion prevention systems.

4.6.1.2. Anti-spoofing filters and controls must be enabled on routers.

4.6.1.3. Network, application, and server authentication passwords are required to meet the same industry standard practices used for the authentication of users set forth in Section 4.3.f above (Authentication). System-level passwords (privileged administration accounts or user- level accounts with privileged administration access) must be changed at minimum every 90 days.

4.6.1.4. Initial user passwords are required to be changed at first log-on. Vertice shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

4.6.1.5. Firewalls must be deployed to protect the perimeter of Vertice's networks.

4.6.2. **Virtual Private Networks ("VPN")**. When using VPN to remotely connect to the Customer's or Vertice's network for processing of Data:

4.6.2.1. Connections must be encrypted using industry standard cryptography.

4.6.2.2. Connections shall only be established using VPN servers.

4.6.2.3. The use of multi-factor authentication is required.

4.6.3. **Data Transfer**. Vertice shall have formal transfer policies in place to protect the transfer of Data through the use of all types of communication facilities that adhere to the requirements of this document. Such policies shall be designed to protect transferred Data from unauthorised interception, copying, modification, corruption, routing and destruction.

4.7. System Acquisition, Development, and Maintenance

4.7.1. **Security Requirements**. Vertice shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

4.7.2. **Development Requirements**. Vertice shall conduct appropriate tests for system security as part of acceptance testing processes.

4.8. Penetration Testing and Vulnerability Scanning & Audit Reports

4.8.1. **Testing**. Vertice will perform periodic vulnerability scans and penetration tests on its internet perimeter network. These scans and tests will be conducted by qualified professionals, including among other entities, Vertice's independent internal compliance team, using industry standard tools and methodologies.

4.8.2. **Audits and Certifications**. Vertice shall cooperate with reasonable requests by Customer for legally required security audits (subject to mutual agreement on the time, duration, place, scope and manner of the audit), and respond to reasonable requests for testing reports. Vertice shall make available to Customer, upon written request and without undue delay, copies of any third party audit reports or certifications it maintains (such as SSAE 16 – SOC1, SOC2, SOC3 attestations or ISO 27001:2013 certifications (or their equivalent under any successor standards)) that apply to the Service, to the extent that Vertice maintains such certifications in its normal course of business. Customer shall treat the contents of reports related to Vertice's security and certifications as confidential information.

4.8.3. **Remedial Action**. If any penetration test or vulnerability scan referred to in Section 4.8.a above reveals any deficiencies, weaknesses, or areas of non-compliance, Vertice shall promptly take such steps as may be required, in Vertice's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable considering Vertice's prioritisation of such, based upon their criticality (e.g. nature, severity, likelihood).

4.8.4. **Status of Remedial Action**. Upon request, Vertice shall keep Customer reasonably informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same.

4.9. Contractor Relationships

4.9.1. **Policies**. Vertice shall have information security policies or procedures for its use of external Representatives that impose requirements consistent with this document.

4.9.2. **Monitoring**. Vertice shall monitor and audit service delivery by its external Representatives and review its external Representatives' security practices against the security requirements set forth in Vertice's agreements with such Representatives.

4.10. Management of Data Breaches and Improvements

4.10.1. **Responsibilities and Procedures**. Vertice shall establish procedures to ensure a quick, effective, and orderly response to Data Breaches.

4.10.2. **Reporting Data Breaches**. Vertice shall implement procedures for Data Breaches to be reported as appropriate. Representatives should be made aware of their responsibility to report Data Breaches as quickly as reasonably possible.

4.10.3. **Reporting Information Security Weaknesses**. Vertice's Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.

4.10.4. **Assessment of Information Security Events**. Vertice shall have classification scale in place in order to decide whether an

information security event should be classified as a Data Breach.

4.10.5. **Response Process**. Vertice shall maintain a record of Data Breaches with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

4.11. Information Security Aspects of Business Continuity Management

4.11.1. **Planning**. Vertice shall maintain emergency and contingency plans for the facilities where Vertice information systems that process Data are located. Vertice shall verify the established and implemented information security continuity controls at regular intervals.

4.11.2. **Data Recovery**. Where and as applicable, Vertice shall design redundant storage and procedures for recovering Data in its possession or control in a manner sufficient to reconstruct Data in its original state as found on the last recorded backup provided by the Customer or in a manner sufficient to resume the Service.

Attachment B

Standard Contractual Clauses (controller to processor)

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

(Text with EEA relevance)

For purposes of this Attachment B: any reference to "data exporter" means Customer and any reference to "data importer" means Vertice (each a "**party**"; together "**the parties**").

The parties have agreed on the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

SECTION I

Clause 1

Purpose and scope

1. 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.
2. The Parties:
3. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex 1.A. (hereinafter each "data exporter"), and
4. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex 1.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

1. These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.
2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

1. 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.
2. 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

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
2. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
3. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3 (b);
4. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
5. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
6. Clause 13;
7. Clause 15.1(c), (d) and (e);

8. Clause 16(e);
9. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
10. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 1.B.

Clause 7

Docking clause

1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A.
2. Once it has completed the Appendix and signed Annex 1.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex 1.A.
3. 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.

MODULE TWO: Transfer controller to processor

1. Instructions
2. 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.
3. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.
4. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.B, unless on further instructions from the data exporter.

1. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex 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 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.

1. 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.

1. Duration of processing and erasure or return of data

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

1. Security of processing

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

3. 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.

4. 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.

5. 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.

6. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1.B.

1. 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:

1. 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;

2. 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;

3. 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

4. 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.

1. Documentation and compliance

2. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

3. 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.

4. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

5. 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.

6. 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

MODULE TWO: Transfer controller to processor

1. GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
2. 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.
3. 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.
4. 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.
5. 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

MODULE TWO: Transfer controller to processor

1. 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.
2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex 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.
3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

1. 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.

MODULE TWO: Transfer controller to processor

1. 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.
2. 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:
3. 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;
4. refer the dispute to the competent courts within the meaning of Clause 18.
5. 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.
6. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
7. 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

MODULE TWO: Transfer controller to processor

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

1. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex 1.C, shall act as competent supervisory authority.

2. 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 practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

3. 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;

4. the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

5. 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.

6. 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.

7. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

8. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

9. 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

MODULE TWO: Transfer controller to processor

1. Notification
2. 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:
3. 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
4. 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.
5. 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.
6. 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.).
7. 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.
8. 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.
9. Review of legality and data minimisation
10. 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).
11. 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.
12. 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

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. 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).
3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
4. 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;
5. the data importer is in substantial or persistent breach of these Clauses; or
6. 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.

1. For Modules One, Two and Three: 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.
2. 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

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of the Republic of Ireland.
3. 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.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

Annex 1 To Attachment B

The Standard Contractual Clauses

This Annex 1 forms part of the Clauses.

A. List of Parties

Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

Data importer

The data importer is Vertice. Activities relevant to the transfer include the performance of services for Customer.

B. Description of transfer

1. **Categories of data subjects whose personal data is transferred**

    1.1. The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of Customer, and other individuals whose personal data is processed by or on behalf of Customer and delivered as part of the Services.

2. **Categories of personal data transferred**

    2.1. The personal data transferred may concern the following categories of data:

    2.2. Personal data related directly or indirectly to the categories of data subjects listed above, including online and offline customer, prospect, and partner data, and personal data provided by or on behalf of the Customer or its users of the Services.

3. **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.**

    3.1. Unless Customer or its users use the Services to transmit or store sensitive data, Vertice does not process sensitive data.

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

    4.1. The Transfer happens on a continuous basis.

5. **Nature of Processing**

    5.1. Personal data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analysing, collecting, transferring, and making available personal data.

6. **Purpose(s) of the data transfer and further processing**

    6.1. The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Vertice and Customer: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under mandatory applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to Customer, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements.

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

    7.1. Personal data will be retained as needed to fulfil the purposes for which it was collected, such as delivery of the Services and Products, and as necessary for Vertice to comply with its business requirements, legal obligations, resolve disputes, protect its assets, and enforce its rights and agreements.

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

    8.1. Personal data will be transferred to Vertice's sub-processors (if any) as described in Annex 3 to Attachment B.

9. **Competent Supervisory Authority**

    9.1. United Kingdom Information Commissioner.

Annex 2 To Attachment B

The Standard Contractual Clauses

Annex 2 to Attachment B, the Standard Contractual Clauses, is the Information Security measures located in Attachment A.

Annex 3 To Attachment B

List of Sub-processors

Name	Purpose	Location	Notes	Link to appropriate safeguards implemented by Subprocessor in case of transfer of personal data to third countries
Amazon Web Services Inc.	Third-party hosting provider and Content Delivery Network, Storage.	Hosting: Ireland (EU) CDN: Cloudfront - Europe and Israel - North America (United States, Mexico, Canada)	Customer Data is stored in Ireland.Customer Data may be transmitted through any CDN region to provide better and faster service response time, depending, for example, on the location of Vertice users when they log in to our Product.	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
ActiveCampaign, LLC (Postmark)	Transactional Emails	United States	Email notifications (e.g contract notifications) sent by the Vertice services are powered Postmark	https://www.activecampaign.com/legal/dpa
Calendly LLC	Meeting scheduler	United States	Meetings are booked through calendar integration using Calendly	https://calendly.com/dpa
Google LLC	Storage and general business services (Email, Documents, Calendar, Analytics, Advertising)	United States		https://business.safety.google/gdpr/
HubSpot, Inc	Internal CRM system, Marketing Automation	United States		https://fs.hubspotusercontent00.net/hubfs/742851/Privacy%20and%20Security%20documents/HubSpot%20Security%20Overview%20-%20October%202021.pdf
Slack Technologies, LLC	Communications	United Kingdom		N/A
Xero Limited	Accounting software	United States		https://www.xero.com/uk/security/
Zoom Video Communications, Inc.	Conferencing	United States		https://explore.zoom.us/en/gdpr/
Atlassian Pty Ltd, Atlassian, Inc	Customer feedback processing and customer support tools	- Asia Pacific (Singapore and Sydney) - Europe (Frankfurt and Ireland) - US (US East and US West)	Atlassian can move data between these locations as required to provide service uptime and integrity	https://www.atlassian.com/trust/privacy/country/europe-and-gdpr
Salesloft, Inc.	Sales engagement	United States		https://salesloft.com/security-compliance/
Box.com (UK) Ltd	Document Storage	United Kingdom	Storage of manually sourced contracts	N/A

Attachment C

UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. This Addendum is effective from the same date as the Clauses.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Clauses those terms shall have the same meaning as in the Clauses. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
The Clauses	The Standard Contractual Clauses set out in Attachment B to the MDPA.
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	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. 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

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

a. for 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 transfer; and

b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 7 above, include (without limitation):

a. References to the "Clauses" means this Addendum as it incorporates the Clauses.

b. 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 1.B to Attachment B where UK Data Protection Laws apply to the data exporter's processing when making that transfer".

c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.

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

e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK".

f. Clause 13(a) and Annex 1.C to Attachment B are not used; the "competent supervisory authority" is the Information Commissioner.

g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

h. Clause 18 is replaced to state:

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

i. The footnotes to the Clauses do not form part of the Addendum.

Amendments to this Addendum

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

11. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.

Executing this Addendum

12. The Parties may enter into the Addendum (incorporating the Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes (but is not limited to):

a. By adding this Addendum to the Clauses and including in the following above the signatures in Annex 1.A to Attachment B:

"By signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated:" and add the date (where all transfers are under the Addendum)

"By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated" and add the date (where there are transfers both under the Clauses and under the Addendum)

(or words to the same effect) and executing the Clauses; or

b. By amending the Clauses in accordance with this Addendum and executing those Clauses.