DATA PROCESSING ADDENDUM

CUSTOMER

This Data Processing Addendum, including all addenda, appendices, attachments and exhibits referenced herein (collectively, the "DPA"), details and outlines Sakon's data processing program.

In the course of providing Sakon's Software-as-a-Service and managed services to Customers, as defined in and pursuant to an addendum, agreement, order, statement of work and/or other contracting document ("Agreement"), Sakon may process personal data and the parties agree to comply with the following provisions with respect to any personal data, each party acting reasonably and in good faith.

Table 1 – Engagement Details (as set forth below or as incorporated from the Agreement) provides information about the Customer and Sakon in relation to the transfer of personal data under this DPA.

Table 1 – Engagement Details	
Data Controller **Data Exporter** **(For this DPA and Annex I)**	[Customer Name in the Agreement] ("Customer" as used herein)
Customer Address **(For this DPA and Annex I)**	[Customer Address from the Agreement]
Details of Privacy Contact at Customer **(For this DPA and Annex I)**	[Customer Contact Name, Title, Email Address from the Agreement]
Data Processor or Sub Processor **Data Importer** **(For this DPA and Annex I)**	Global Sourcing Group Inc. d/b/a Sakon ("Sakon" as used herein) 300 Baker Avenue, Suite 280 Concord, MA 01742 (USA) Anis Shaikh – Vice President anis.shaikh@sakon.com
Sub-Processor(s) and services provided by the Sub-Processor(s) **(For this DPA and Annex III)**	None unless otherwise specified in this DPA or in Sakon's contract with the Customer.

By signing this DPA and/or by signing an Agreement that incorporates this DPA (whether incorporated internally within the Agreement, as an addendum, attachment or exhibit to the Agreement, or by incorporation through a web link), Sakon and the Customer accept this DPA (including the details and designations provided in Table 1 – Engagement Details in the Agreement and/or in this DPA, agree to be bound by its terms, and incorporate it into the subject Agreement. Although this DPA indicates that signatures are required in certain areas, Sakon and Customer agree that such signatures are not necessary, as their signatures on the subject Agreement indicates their acceptance of, agreement to and incorporation of this DPA into the subject Agreement. In the event of a conflict with the Agreement, this DPA shall prevail over the Agreement.

1. DEFINITIONS.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1.1. "**Adequate Country**" means a country or territory recognised as providing adequate protection for Personal Data under an adequacy decision or regulations made from time to time by (as applicable) (i) the European Commission under the EU GDPR, ii) the UK Secretary of State under the UK GDPR or iii) the Swiss Federal Data Protection Authority under Swiss Data Protection Law.

1.2. “**Affiliate**” includes all entities, now or hereafter, controlling, controlled by, or under common control with, Sakon. For the purpose of this definition, “control” or “controlled” means direct or indirect ownership of fifty percent (50%) or more of the shares of stock entitled to vote for the election of directors in the case of a corporation or fifty percent (50%) or more of the equity interest in the case of any other type of legal entity; status as a general partner in any partnership; or any other arrangement whereby the entity or person controls or has the right to control the board of directors or equivalent governing body of a corporation or other entity or the ability to cause the direction of the management or policies of a corporation or other entity.

1.3. “**CCPA**” means the California Consumer Privacy Act of 2018 (CCPA), as amended.

1.4. “**Customer**” means the customer or client identified in the Agreement or Statement of Work.

1.5. “**Customer Data**” means the electronic data or information submitted by Customer or Authorized Parties to the Service.

1.6. "**Data Controller**" or “**Controller**” means an entity that determines the purposes and means of the processing of Personal Data.

1.7. "**Data Processor** “or “**Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

1.8. “**Data Protection Laws**” means EU GDPR, the UK GDPR, the California Consumer Protection Act (“CCPA”), the Privacy and Electronic Communications (EC Directive) Regulations 2003, Swiss Data Protection Law and the Security of Network & Information Systems Regulations 2018, all as amended and/or replaced, and in force from time to time and all applicable laws and regulations governing data privacy.

1.9. “**DPA**” means this Data Processing Addendum to the Agreement.

1.10. “**DPA Exhibit**” means an exhibit of the Customer Addendum that describes the customer specific data, data subjects, processing activities, any “pass-through” Customer obligations with respect to processing Customer's Personal Data, and other required elements of the Data Protection Laws and contains the "Standard Contractual Clauses".

1.11. "**EEA**" means the European Economic Area.

1.12. "**EU GDPR**" means General Data Protection Regulation, 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/ECa.

1.13. "**Personal Data**" means any information relating to an identified or identifiable natural person.

1.14. "**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.

1.15. "**Restricted Transfer**" means a transfer of Personal Data processed by Sakon pursuant to this DPA and to which EU GDPR, the UK GDPR or Swiss Data Protection Law applies to a territory other than an Adequate Country and which transfer would be prohibited by EU GDPR or UK GDPR (as appropriate) in the absence of a transfer mechanism recognised by EU GDPR or UK GDPR (as appropriate).

1.16. "**Standard Contractual Clauses**" means module 2 (controller-to-processor) of the Standard Contractual Clauses that are required under Data Protection Laws as set out at Appendix I of this DPA, including Annexes I – III of Appendix I.

1.17. "**Sub-processor**" means any entity engaged by a Processor or another sub-processor who agrees to process Personal Data on such Processor's behalf for the benefit of and in accordance with instructions of the applicable Controller, per the terms of a written subcontract between Processor and Sub-processor, and in compliance with Data Processing Laws.

1.18. "**Swiss Data Protection Law**" means the Swiss Federal Data Protection Act of 19 June 1992 and, when in force, the Swiss Federal Data Protection Act of 25 September 2020 and its corresponding ordinances as amended, superseded or replaced from time to time.

1.19. "**Swiss Addendum**" means the addendum set out at Appendix 3 of this DPA.

1.20. "**UK Approved Addendum**" means the template Addendum B.1.0 and the accompanying mandatory clauses as issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, in force from 21 March 2022, as set out at Appendix 2 of this DPA.

1.21. "**UK GDPR**" means EU GDPR as implemented into the law of the United Kingdom by the

Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020 and the Data Protection Act 2018.

2. SCOPE AND APPLICABILITY OF THIS DPA.

2.1. Scope and Applicability. This DPA applies where and only to the extent that Sakon processes Customer Personal Data: (1) that originates from the EEA and/or that is otherwise subject to EU GDPR, UK GDPR or Swiss Data Protection Law, and where Sakon is acting on behalf of and as processor for Customer in the course of providing Services pursuant to the Agreement or any Order, or (2) Sakon processes Personal Data subject to the CCPA.

2.2. Details of the Processing. The subject-matter of Processing of Personal Data by Sakon is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data (including special categories of personal data), any “flow-through” obligations passed on to Sakon acting as Processor of Personal Data, and categories of Data Subjects Processed under this DPA are further specified in Data Processing Exhibit (Details of the Processing) of any Customer Addendum.

2.3. Roles of the Parties. The parties acknowledge and agree that regarding the Processing of Personal Data, Customer is the Data Controller and Sakon is the Processor of Customer’s Personal Data.

2.4. Compliance. Each party will comply with the obligations applicable to it under the Data Protection Laws with respect to the processing of that Personal Data.

3. DATA PROCESSING.

3.1. Sakon’s Processing of Personal Data. Sakon shall, in its deployment and operation of the Services, process Personal Data (if applicable) in accordance with the requirements of Data Protection Laws. For the avoidance of doubt, any instructions from Customer for the processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquired Personal Data.

3.2. Compliance with Privacy Laws. Customer agrees to comply with all Data Protection Laws applicable to Customer as the “Controller” of any Personal Data provided hereunder. Sakon agrees that, as between the parties, Customer shall be responsible for obtaining any required written consent, affirmative opt-in or other written authorization (“Consent") from applicable individuals in the European Union with respect to their Personal Data, or determining another legitimate, legal basis for processing of such Personal Data. Customer assures Sakon that it will make such Personal Data accessible to Sakon, and also for onward transfer of this data as required by the Order or as otherwise necessary for performance of the Services.

3.3. Processing of Personal Data. Sakon shall treat Personal Data as Confidential Information and shall only process Personal Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Addenda; (ii) Processing initiated by End Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3.4. Instructions. This DPA, an Agreement and any written instructions from Customer to Sakon, are Customer's complete instructions to Sakon for the processing of EU/UK/California personal data related to the Services. Any alternative or additional instructions may only be by written amendment to this DPA sent to the address below or via email from Customer. Sakon will receive notice of any alternative or additional instructions as applicable in accordance with the notice provisions of the subject Agreement.

3.5. Authority. Customer will have the exclusive authority to determine the purpose for and means of processing EU/California personal data.

3.6. Compliance. Sakon shall comply with all applicable Data Protection Laws, including but not limited to, the EU GDPR, the UK GDPR, Swiss Data Protection Laws and the CCPA (see Appendix 4 to this DPA), with respect to all processing it conducts on Customer Personal Data which it undertakes per any Order, this DPA and the Agreement, as well as to the extent such laws apply to Sakon in its role as a processor. Additionally, in its role as processor for Customer, Sakon agrees:

(a) if the EU GDPR or the UK GDPR applies to the processing of Personal Data, the data protection obligations set out in Article 28(3) of the EU GDPR or UK GDPR, as described in these Terms, are imposed on Sakon as processor; and

(b) it only accesses and uses Personal Data to the extent required to perform the obligations subcontracted to it and does so in accordance with the Agreement (including these Terms).

3.7. Data Protection Impact Assessment. Upon Customer's request, Sakon shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the EU GDPR or UK GDPR to carry out a data protection impact assessment related to Customer's use of the Services.

4. RIGHTS OF DATA SUBJECTS.

4.1. Data Subject Request. Sakon shall, to the extent legally permitted, promptly notify Customer if Sakon receives a request from a Data Subject, to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request").

4.2. Assistance. Accounting for the nature of the Processing, Sakon shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Sakon's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the

Services, does not have the ability to address a Data Subject Request, Sakon shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Sakon is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Sakon's provision of such assistance.

5. RETURN OR DELETION OF DATA.

5.1. Return or Deletion. Upon termination or expiration of the Agreement, Sakon shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, provided that this requirement shall not apply to the extent Sakon is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Sakon shall securely isolate and protect from any further processing, except to the extent required by applicable law.

6. TRACKING TECHNOLOGIES.

6.1. Tracking Technologies. Sakon acknowledges that in connection with the performance of the Services, Sakon employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Company will be responsible for shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable Sakon to deploy Tracking Technologies lawfully on, and collect data from, the devices of end users in accordance with and as described in the Sakon Privacy Notice.

7. SUB-PROCESSING.

7.1. Appointment of Authorized Sub-processors. Sakon may engage Sub-processors.

7.2. Sub-processor Obligations. When engaging any Sub-processor, Sakon will ensure via a written contract that:

(a) the Sub-processor only accesses and uses Personal Data to the extent required to perform the obligations subcontracted to it and does so in accordance with the Agreement (including these Terms)

(b) if the EU GDPR or UK GDPR applies to the processing of Personal Data, the data protection obligations set out in Article 28(3) of the EU GDPR or UK GDPR, as described in these Terms, are imposed on the Subprocessor; and

(c) Sakon will remain responsible for its compliance with the obligations of this DPA, the Agreement and any related Order, and for any acts or omissions of the Sub-processor that cause Sakon to breach any of its obligations under this DPA, the Agreement, or related Order.

(d) Written agreements with each Sub-processor shall contain data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

7.3. List of Current Sub-processors and Notification of New Sub-processors.

(a) Sakon shall make available to Customer the current list of Sub-processors for the Services identified in this DPA or in Sakon's contract with the Customer.

(b) Sakon shall provide written notification of a new Sub-processor(s) before authorizing any new Subprocessor(s) to Process Personal Data in connection with the provision of the applicable Services.

(c) Customer may object to Sakon's use of a new Sub-processor by notifying Sub-processor promptly in writing within ten (10) business days after receipt of Sakon's notice.

(d) Methods of notices, referenced in Section 3.4, shall follow the notice provisions of the subject Agreement.

7.4. Liability. Sakon shall be liable for the acts and omissions of its Sub-processors to the same extent Sakon would be liable if performing the services of each Sub-processor directly under the terms of this Data Protection Addendum, except as otherwise set forth in the Agreement.

8. SECURITY MEASURES.

8.1. Security Measures. Sakon will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access in accordance with Sakon's security standards, including, as appropriate, the measures required pursuant to Article 32 of the EU GDPR or the UK GDPR.

8.2. Confidentiality of Processing. Sakon shall ensure that any person who is authorized by Sakon to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality.

8.3. Personnel. Sakon shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and have received appropriate training on their responsibilities.

9. LIMITATION OF ACCESS.

9.1. Limitation. Sakon shall ensure that Sakon's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

9.2. Security Certifications and Reports. Sakon shall ensure the continued effectiveness of the security measures.

9.3. Customer's Audit Rights. If EU GDPR or UK GDPR applies to the processing of Personal

Data, Sakon will allow Customer or an independent auditor appointed by Customer or Sakon to conduct audits (including inspections) to verify Sakon's compliance with its obligations under these Terms.

9.4. Verification. Customer may also conduct an audit to verify Sakon's compliance with its obligations under these Terms by reviewing Sakon's documentation outlining its security measures.

10. INCIDENT MANAGEMENT.

10.1. Policies. Sakon maintains security incident management policies and procedures in accordance with EU GDPR or UK GDPR.

10.2. Security Incident Response. Upon becoming aware of a security incident, Sakon shall notify Customer without undue delay and shall provide timely information relating to the security incident as it becomes known or as is reasonably requested by Customer. Sakon shall make reasonable efforts to identify the cause of such security incident and take those steps as Sakon deems necessary and reasonable in order to remediate the cause of such security incident to the extent the remediation is within Sakon's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer. Should Customer incur expenses as a result of a security incident attributable to Sakon, Sakon shall indemnify Customer for said expenses.

10.3. No Acknowledgement of Fault by Sakon. Sakon's notification of or response to a security incident under this Section will not be construed as an acknowledgement by Sakon of any fault or liability with respect to the security incident.

10.4. Customer Responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials and, in cases when Personal Data is being transmitted from Customer to Sakon, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

11. INTERNATIONAL TRANSFERS.

11.1. To the extent that any Restricted Transfer is subject to the EU GDPR, the parties agree that the Standard Contractual Clauses approved by the EU authorities under Data Protection Laws and set forth at Appendix 1 to this DPA and Annexes I, II and III to the Standard Contractual Clauses shall apply in respect of that processing.

11.2. To the extent that any Restricted Transfer is subject to the UK GDPR, the parties agree that the UK Approved Addendum as set forth at Appendix 2 to this DPA shall apply in respect of that processing.

11.3. To the extent that any Restricted Transfer is subject to Swiss Data Protection Law, the parties agree that the Swiss Addendum set forth at Appendix 3 to this DPA shall apply in respect of that processing.

11.4. Standard Contractual Clauses. The Standard Contractual Clauses are in the Data Processing Exhibit Appendix 1.

12. MISCELLANEOUS.

12.1. This DPA, or any subsequent version of this DPA as updated by Sakon, shall remain in full force and effect throughout the Agreement.

12.2. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations of liability set forth in the Agreement.

12.3. Customer may terminate this DPA and the Standard Contractual Clauses at Customer's discretion upon Sakon's receipt of Customer's written notice of termination.

12.4. This DPA (other than the SCCs, the UK Transfer Addendum and the Swiss Addendum) will be governed by and construed in accordance with governing law and jurisdiction provisions set forth in the Agreement, unless otherwise required by applicable privacy laws.

DATA PROCESSING EXHIBIT (GDPR)

This Exhibit includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

1. **SUBJECT MATTER**. The subject matter and duration of the processing of Personal Data are setout in the Agreement.

2. **DURATION OF PROCESSING**. The Term specified in the Agreement plus the period from the expiry of the Termination of Agreement until deletion of all Customer Data by Sakon in accordance with the terms of the agreement.

3. **NATURE AND PURPOSE OF THE PROCESSING**. Sakon will process Personal Data for the purposes of providing the Sakon Services to Customer in accordance with the Agreement.

4. **TYPE OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECT TO BE PROCESSED**.

   - Customer's employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants)
   - Customer's affiliates employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants)
   - Customer's business partners (if those business partners are individuals)
   - Employees of Customer's business partners
   - Customer's suppliers and subcontractors (if those suppliers and subcontractors are individuals)
   - Employees of Customer's suppliers and subcontractors
   - Customer's agents, consultants and other professional experts (contractors)

5. **CATEGORIES OF DATA TO WHOM THE COMPANY PERSONAL DATA RELATES**. Client may submit Personal Data to the Sakon Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

   - Person Name
   - Online Access and Authentication Credentials
   - Telephony
   - Consumed Resources
   - Online Identifier
   - Technology Identifiers
   - Profession and Employment Information
   - Appointments, Schedules, Calendar Entries
   - Physical Location of the Individual
   - Individual's manager/supervisor information

6. **THE OBLIGATIONS AND RIGHTS OF COMPANY AND COMPANY AFFILIATES**. The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this DPA.

APPENDIX 1: STANDARD CONTRACTUAL CLAUSES

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

STANDARD CONTRACTUAL CLAUSES

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) ([1]) for the transfer of personal data to a third country.

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

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

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   (ii) Clause 8 – 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);

   (iii) Clause 9 – MODULE TWO: Clause 9(a), (c), (d) and (e); MODULE THREE: Clause 9(a), (c), (d) and (e);

   (iv) Clause 12 – MODULE ONE: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

   (v) Clause 13;

   (vi) Clause 15.1(c), (d) and (e);

   (vii) Clause 16(e);

   (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); MODULE FOUR: Clause 18.

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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 Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these

Clauses, in particular purpose limitation.

8.9 Documentation and compliance

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

b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

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

d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter’s prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 10 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

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

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

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

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

Clause 10

Data subject rights

a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

Clause 13

Supervision

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

b) 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

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

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

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

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

f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

  (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

  (ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

(iv) 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

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

a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b) The Parties agree that those shall be the courts of the Republic of Ireland.

c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES. For the information outlined below, see Table 1 – Engagement Details, which appears in the Agreement, Statement of Work and/or this DPA, and which is incorporated into this Section A as appropriate.

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: ____

Address: ____

Contact person's name, position and contact details: ____

Activities relevant to the data transferred under these Clauses:

Receipt of the Services____

Signature and date: ____

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: ____

Address: ____

Contact person's name, position and contact details: ____

Activities relevant to the data transferred under these Clauses:

Delivery of the Services

Signature and date: ____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Customer's employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants)
- Customer's affiliates employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants)
- Customer's business partners (if those business partners are individuals)
- Employees of Customer's business partners
- Customer's suppliers and subcontractors (if those suppliers and subcontractors are individuals)
- Employees of Customer's suppliers and subcontractors

- Customer's agents, consultants and other professional experts (contractors)

Categories of personal data transferred

- First and last name
- Individual
- Online Access and Authentication Credentials
- Telephony
- Consumed Resources
- Online Identifier
- Person Name
- Technology Identifiers
- Profession and Employment Information
- Appointments, Schedules, Calendar Entries
- Physical Location of the Individual

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.

N/A

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

Continuous

Nature of the processing

Collecting, Recording, Organizing, Storage, Use, Alteration, Disclosure, Transmission, Retrieval, Destruction, Archival

Purpose(s) of the data transfer and further processing

Delivery of the Services

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

Duration of the Agreement.

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

As stated above.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority under Clause 13 shall be the EU or UK supervisory authority with responsibility for ensuring compliance by the Data Exporter

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Data Importer maintains a written security program for the security, integrity and protection of personal data it processes on behalf of its customers against unauthorized disclosure and loss. Data Importer's security program includes administrative, technical and physical safeguards appropriate for data importer's size and resources and the types of information that it processes. Technical and organizational security measures, including administrative, physical, and technical safeguards relation to our Processing of Your Personal Data can be found at **http://www.Sakon.com/security-measures**

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors (see Table 1 – Engagement Details in this DPA or in Sakon's contract with the Customer for requisite information about sub-processors engaged for this matter, if any):

APPENDIX 2
UK TRANSFER ADDENDUM

UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the UK Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

For the details below, see Table 1 – Engagement Details, which is located in the Agreement, Statement of Work and/or this DPA.

Start date	The Effective Date of the DPA between the Parties.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: *The Exporter is the Customer* Trading name (if different): [*parties to complete if applicable*] Main address (if a company registered address): Official registration number (if any) (company number or similar identifier): [*parties to insert*]	Full legal name: *The Importer is Sakon* Trading name (if different): *N/A* Main address (if a company registered address): *Sakon's address is set out in the DPA* Official registration number (if any) (company number or similar identifier): *As set out in the DPA*
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)	Executed in accordance with this DPA	Executed in accordance with this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ 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?
1						
2	√	√	x	Specific Authorisation	10 days	No
3						
4						

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: *See the DPA*
Annex 1B: Description of Transfer: *See Annex I of Appendix 1 of the DPA*

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: *See Annex II of Appendix 1 the DPA*
Annex III: List of Sub processors (Modules 2 and 3 only): *See Annex III of Appendix 1 the DPA*

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 ☒ Neither Party

Part 2: Mandatory Clauses

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.

Alternative Part 2 Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.

APPENDIX 3: SWISS ADDENDUM

In respect of Restricted Transfers to which Swiss Data Protection Law applies:

- The FDPIC will be the competent supervisory authority;
- Data subjects in Switzerland may enforce their rights in Switzerland under Clause 18c of the EU Standard Contractual Clauses, and
- References in the EU Standard Contractual Clauses to the EU GDPR should be understood as references to Swiss Data Protection Law insofar as the data transfers are subject to Swiss Data Protection Law.

APPENDIX 4:

CCPA ADDENDUM

Restrictions on Use and Disclosure.

1. To the extent the CCPA is applicable, Sakon's compliance statement with regard to the CCPA is set forth on Sakon's website at the following page: https://www.sakon.com/privacy-policy ("CCPA Policy"). Such page is incorporated herein by reference.

2. In general, and as more clearly set forth in the CCPA policy, for purposes of Personal Data that is Personal Information as defined in and subject to the CCPA, as between Sakon and Service Provider:

    a. Sakon is a "processor" or subprocessor" and Customer is a "data controller" (each as defined in the CCPA):

    b. Sakon will not retain, use, or disclose such Personal Data for any purpose other than as required for the specific purpose of performing the services, and to detect security incidents and protect against illegal activity.

    c. Sakon will not "sell" such Personal Data to any third party. For these purposes, "sell" has the meaning ascribed to it in the CCPA.

    d. For clarity, the restrictions in this Annex 4 include retention, use or disclosure of such Personal Sakon outside of the direct business relationship between Sakon and Customer.

3. Sakon understands the restrictions in this Annex 4 and will comply with them.

In the event of any conflict between the terms of this CCPA Addendum and the terms of the Main Agreement or CCPA Policy, the terms of the CCPA Policy will prevail so far as the subject matter concerns the processing of Personal Data under the CCPA. Except as otherwise set forth in this CCPA Addendum, the Main Agreement, DPA and CCPA Policy remain unchanged and in full force and effect.