

THIS ADDENDUM is made on the same date as the Master Services Agreement

BETWEEN:

- (1) Customer as described in the Master Services Agreement between Customer and LogiSense Corporation (the “**Customer**”); and
 - (2) **LOGISENSE CORPORATION**, a corporation incorporated pursuant to the laws of Ontario, Canada, with its registered address at 278 Pinebush Drive, Unit 101, Cambridge, Ontario, Canada, N1T 1Z6 (the “**LogiSense**”)
- (each a “**Party**” and together the “**Parties**”).

WHEREAS:

- (A) The Customer and LogiSense have entered into a Master Services Agreement (the “**Agreement**”).
- (B) In the course of providing services under the Agreement, LogiSense processes personal data on behalf of the Customer.
- (C) The Parties wish to amend the Agreement with effect from the date of the Agreement (the “**Effective Date**”) by adding the terms set out in this Addendum, which is supplemental to the Agreement.

NOW IT IS AGREED AS FOLLOWS:

1. Supplemental Terms

1.1 With effect from the Effective Date, the following terms shall form part of the Agreement:

1. Data Protection

1.1 For the purposes of this clause:

“**Data Protection Law**” means all applicable data protection law, including the General Data Protection Regulation (Regulation (EU) 2016/679), the Data Protection Act 2018 of the United Kingdom (the “**Data Protection Act**”) and the UK General Data Protection Regulation and any legislation which amends, extends, consolidates, re-enacts or replaces same, including any statutory instruments and regulations that may be made pursuant thereto from time to time.

“**Standard Contractual Clauses**” means, as applicable the standard contractual clauses for the transfer of personal data to processors in third countries adopted by the European Commission under Decision (EU) 2021/914 and the standard data protection clauses issued by the Commissioner under S119A(1) of the Data Protection Act.

The terms ‘**controller**’, ‘**personal data**’, ‘**personal data breach**’, ‘**processor**’ and ‘**process**’ shall have the meanings given to them under Data Protection Law.

1.2 LogiSense acknowledges that in performing its obligations under the Agreement LogiSense processes personal data on behalf of the Customer. In such circumstances, LogiSense acknowledges that the Customer is the controller or a processor acting on behalf of the controller and LogiSense is a processor or sub-processor, as each term is defined in Data Protection Law.

- 1.3 LogiSense shall process the categories of personal data set out in the Appendix to this Addendum in the context of performing its obligations under, and for the duration of, the Agreement. The obligations and rights of the Customer shall be as set out in this Addendum.
- 1.4 In respect of the personal data referred to in Clause 1.3:
- (a) LogiSense shall process such personal data only in accordance with the documented instructions of the Customer, including with regard to transfers of personal data to a third country and solely as necessary for the performance of its obligations under the Agreement, unless required to do so by EU or EU Member State law to which LogiSense is subject, or by UK law, as applicable, in which case LogiSense shall inform the Customer of that legal requirement before processing (unless that law prohibits such information on important grounds of public interest);
 - (b) LogiSense shall ensure that the persons authorised by LogiSense to process such personal data are bound by appropriate confidentiality obligations;
 - (c) LogiSense shall implement such technical and organisational security measures as are required to comply with the data security obligations under Data Protection Law, which may include, as appropriate:
 - (i) the pseudonymisation and encryption of personal data;
 - (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
 - (d) LogiSense is authorised to engage sub-processors to undertake processing on its behalf (see section 1.5(f) of this Addendum), provided that it provides the Customer with prior notice in writing containing details of the sub-processors that it engages and informs the Customer of any intended changes concerning the addition or replacement of such sub-processors and provides the Customer with a reasonable opportunity to object to such changes;
 - (e) where any sub-processor engaged by LogiSense will be processing such personal data, LogiSense shall ensure that a written contract exists between LogiSense and the sub-processor containing clauses equivalent to those imposed on LogiSense in this clause. In the event that any sub-processor fails to meet its data protection obligations, LogiSense shall remain fully liable to the Customer for the performance of the sub-processor's obligations;
 - (f) LogiSense shall assist the Customer by implementing appropriate technical and organisational measures to allow the Customer to comply with requests from data subjects to exercise their rights under Data Protection Law;
 - (g) LogiSense shall, at the cost and expense of the Customer, assist the Customer in ensuring compliance with applicable obligations in respect of security of

personal data, data protection impact assessments, and prior consultation requirements under Data Protection Law;

- (h) LogiSense shall: (i) at the choice of the Customer, delete or return all such personal data to the Customer when LogiSense ceases to provide services relating to data processing; and (ii) delete all existing copies of such personal data unless EU law or the laws of an EU Member State, UK law, as applicable require storage of the personal data;
- (i) LogiSense shall: (i) make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in this clause; and (ii) at the cost and expense of the Customer, allow for and assist with audits, including inspections, conducted by the Customer or another party mandated by the Customer, in order to ensure compliance with the obligations laid down in this clause, including its data security obligations under Data Protection Law. The Customer shall take into account adherence by LogiSense to an approved code of conduct or an approved certification mechanism to aid demonstration by LogiSense that it is compliant with the provisions of this clause;
- (j) LogiSense shall inform the Customer immediately if, in its opinion, it receives an instruction from the Customer in connection with clause 1.4(i) which infringes Data Protection Law; and
- (k) LogiSense shall notify the Customer without undue delay after becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, such personal data and shall provide the Customer with such co-operation and assistance as may be reasonably required to comply with any notification or reporting obligations which may apply in respect of, any such personal data breach.

1.5 It is acknowledged and agreed that LogiSense shall process personal data outside the European Economic Area and/or the United Kingdom in one or more 'third countries' for the purpose of Chapter V of the GDPR which has not been deemed by the European Commission and/or the United Kingdom's Information Commissioner's Office to ensure an adequate level of protection for personal data. The transfer of personal data from the Customer to LogiSense in these circumstances shall be governed by, as applicable, (i) both sets of Standard Contractual Clauses, (i) the EU Standard Contractual Clauses, or (ii) the UK Standard Contractual Clauses, which are hereby incorporated into this Addendum. In case of conflict between this Addendum and the applicable Standard Contractual Clauses, the applicable set of Standard Contractual Clauses shall apply to the personal data. For the purpose of the Standard Contractual Clauses:

- (a) the data exporter's name, address and contact details shall be those of the Customer;
- (b) the data importer's name, address and contact details shall be those of LogiSense;
- (c) the Customer hereby consents to LogiSense sub-contracting any of its processing operations performed on behalf of the Customer, provided that it shall comply with the requirements of this Addendum and the Standard Contractual Clauses in connection therewith;

- (d) for the purpose of Annex I to the EU Standard Contractual Clauses the personal data (and special categories of personal data, if any) transferred, the categories of data subjects to whom the personal data relate and the processing activities that shall take place in respect of such personal data are as set out or referenced in the Annex I to the Standard Contractual Clauses
- (e) for the purpose of Annex II to the EU Standard Contractual Clauses and Annex I of the UK Standard Contractual Clauses, the technical and organisational security measures that shall be implemented by LogiSense shall be the security measures set out or referenced in Annex II to the EU Standard Contractual Clauses and Annex I to the UK Standard Contractual Clauses; and
- (f) for the purpose of Clause 9 of the EU Standard Contractual Clauses, the list of agreed-upon sub-processors is set forth in Annex III to the EU Standard Contractual Clauses; for the purpose of Table 2 “Specific restrictions when the Importer may transfer on the Transferred Data” of the UK Standard Contractual Clauses, the list of agreed-upon sub-processors is set forth in Annex II to the UK Standard Contractual Clauses.

2. **Miscellaneous**

- 2.1 Capitalised terms not otherwise defined in this Addendum shall have the meanings set forth in the Agreement.
- 2.2 Save to the extent explicitly amended by this Addendum, the Agreement shall continue in full force and effect. To the extent that there is a conflict or inconsistency between the terms of this Addendum and the Agreement, such conflict or inconsistency shall be resolved by giving precedence to this Addendum.
- 2.3 This Addendum and the Agreement shall together constitute the entire agreement between the Parties with respect to their subject matter, supersede all previous drafts, arrangements, understandings or agreements between the Parties with respect to their subject matter and may not be modified except by an instrument in writing signed by the duly authorised representatives of the Parties. Each of the Parties acknowledges and agrees that in entering into this Addendum it does not rely on and shall have no remedies in respect of, any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this Addendum or not) relating to the subject matter of this Addendum, other than as expressly set out in this Addendum.
- 2.4 This Addendum may be executed in any number of counterparts, each of which when executed and delivered by one or more of the Parties to this Addendum is an original, but all the counterparts together constitute the same document provided that this Addendum shall not be effective until each party has executed and delivered at least one counterpart. The Parties agree that this Addendum may be executed electronically. Transmission of an executed counterpart of this Addendum (but for the avoidance of doubt not just a signature page) by (a) fax or (b) email (in PDF, JPEG or other agreed format) shall also constitute delivery of an executed counterpart of the Addendum.
- 2.5 This Addendum shall be governed by and construed in accordance with the laws of the governing law of the Agreement.

EU 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 Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

- (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);
- (iv) Clause 12 – Modules Two: 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).

(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 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 (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)

GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list, as set forth in Annex III. 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 7 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 ac involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose processing; the categories and format of the transferred personal data; the economic sector in which 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 dat public authorities or authorising access by such authorities – relevant in light of the specific circumstar of the transfer, and the applicable limitations and safeguards ⁽¹²⁾;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguar under these Clauses, including measures applied during transmission and to the processing of the perso 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 law of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; notification shall include information about the personal data requested, the requesting authority, the 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 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.). [For Module Three: The data exporter shall forward the information to the controller.]
- (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 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

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]*

1. Name: ...
Address: ...
Contact person's name, position and contact details: ...
Activities relevant to the data transferred under these Clauses: ...
Signature and date: ...
Role (controller/processor): ...

2. ...

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

1. Name: LogiSense Corporation
Address: 278 Pinebush Rd #101, Cambridge, N1T 1Z7
Kevin Fox, Director, Security & Technical Operations; kfox @logisense.com
Activities relevant to the data transferred under these Clauses: collection, preparation, input, processing, output, storage
Signature and date: ...
Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Customers and customers' end users

Categories of personal data transferred

- Name
- Address
- Call data
- Usage data

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.

- No sensitive data
- For additional clarity, Customer agrees that it will not make available the following categories of information to LogiSense: government issued personal identification numbers, consumer financial account information, credit and payment card information, personal health information, or information deemed "sensitive" under applicable Data Protection Law (such as racial or ethnic origin, political opinions, or religious or philosophical beliefs) except with LogiSense's prior written approval. For the purpose of clarity examples of government issued personal identification numbers are drivers' license numbers, Social Security Numbers (U.S)/ Social Insurance Number (Canada) or the equivalent in the European Union, passport numbers, etc., but not information that is typically included in billing systems such as taxation numbers, company numbers, address, etc.

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

- Call and Usage data is transferred continuously

Nature of the processing

- Call and Usage Cost Calculation

Purpose(s) of the data transfer and further processing

- Customer Billing

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

Data importer retains the personal data until the expiration or termination of the services agreement between data importer and data exporter.

...

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

...

ANNEX II

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

MODULE TWO: Transfer controller to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer has a thorough suite of information security policies that are based on the SSAE18, PCIDSS information security standards and GDPR, and include policies related to:

Acceptable Use

Access Control

Change Management

Endpoint Security

Information Classification

Human Resource Security

Logging and Monitoring

Operations Backup

Password

Physical and Environment Security

Security Incident Management

Security Risk Management

Security Vulnerability Management

Third-Party Risk Management

Wireless Security

The foundation of these policies is the principle that data is accessed only as required and they are anchored in the key concepts of least-privilege, need-to-know, and segregation of duties. Data importer reviews these policies annually or as required, including upon the occurrence of a significant change to its business process or environment, or to applicable legislation.

Verification of Security Controls

Data importer performs internal testing of key security and privacy controls to verify its compliance with established internal frameworks, including third party security penetration testing on an annual basis. The results of this internal testing are then shared with executive management as applicable; any required substantive remediation efforts are then monitored and controls are re-tested, as required, to ensure compliance with established internal frameworks.



On an semi-annual basis, an independent third party audits data importer's security and privacy controls to verify that the required technology, processes and procedures are in place, and that such processes and procedures are being followed.

A summary of our SOC 1 Type II report may be requested through your account manager.

ANNEX III
LIST OF SUB-PROCESSORS

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

Sub-Processor	Purpose	Country	DPA Reference
Amazon Web Services Inc.	Applicaiton Cloud infrastructure	USA	https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/#:~:text=Data%20Processing%20Addendum(.pdf
Spreadly	Payment Processing and Gateway Integration	USA	https://www.spreadly.com/gdpr#:~:text=of%20which%20is-,hosted%20here.,-This%20DPA%20provides
Workato	Workflow and Integration Automation	USA	https://www.workato.com/legal/dpa
Critical River	Implementation and Onboarding Services	USA	
Anita Middleton LLC	Technical Support services for the platform	USA	

UK STANDARD CONTRACTUAL CLAUSES

VERSION A1.0, in force 21 March 2022

This IDTA has been issued by the 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 and signatures

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: LogiSense Corporaton Trading name (if different): Main address (if a company registered address): 278 Pinebush Rd #101, Cambridge, ON, N1T 1Z6 Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Kevin Fox Job Title: Director, Security & Technical Operations Contact details including email: kfox@logisense.com
Importer Data Subject Contact		Job Title: Director, Security & Technical Operations Contact details including email: kfox@logisense.com
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the Exporter set out above Signed: Date of signature: Full name: Job title:	Signed for and on behalf of the Importer set out above Signed: Date of signature: Full name: Kevin Fox Job title: Director, Security & Technical Operations

Table 2: Transfer Details

UK country's law that governs the IDTA:	<input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
Primary place for legal claims to be made by the Parties	<input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: <input checked="" type="checkbox"/> Exporter is a Controller <input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Importer is a Controller <input checked="" type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor <input type="checkbox"/> Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	<input checked="" type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data <input type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	<p>If the Importer is the Exporter's Processor or Sub-Processor – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:</p> <p>Name of agreement:</p> <p>Date of agreement:</p> <p>Parties to the agreement:</p> <p>Reference (if any):</p> <p>Other agreements – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:</p> <p>Name of agreement:</p> <p>Date of agreement:</p> <p>Parties to the agreement:</p> <p>Reference (if any):</p> <p>If the Exporter is a Processor or Sub-Processor – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:</p>

	<p>Name of agreement:</p> <p>Date of agreement:</p> <p>Parties to the agreement:</p> <p>Reference (if any):</p>
Term	<p>The Importer may Process the Transferred Data for the following time period:</p> <p><input checked="" type="checkbox"/> the period for which the Linked Agreement is in force</p> <p><input type="checkbox"/> time period:</p> <p><input type="checkbox"/> (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.</p>
Ending the IDTA before the end of the Term	<p><input checked="" type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.</p> <p><input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving: <input type="checkbox"/> months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).</p>
Ending the IDTA when the Approved IDTA changes	<p>Which Parties may end the IDTA as set out in Section 29.2:</p> <p><input checked="" type="checkbox"/> Importer</p> <p><input checked="" type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
Can the Importer make further transfers of the Transferred Data?	<p><input checked="" type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p> <p><input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p>
Specific restrictions when the Importer may transfer on the Transferred Data	<p>The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:</p> <p><input type="checkbox"/> if the Exporter tells it in writing that it may do so.</p> <p><input checked="" type="checkbox"/> to: Annex II – List of Sub-Processors to Whom Importer May Transfer on the Transferred Data</p> <p><input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in:</p> <p><input type="checkbox"/> there are no specific restrictions.</p>

Review Dates	<input type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: The Parties must review the Security Requirements at least once: <input type="checkbox"/> each [] month(s) <input type="checkbox"/> each quarter <input type="checkbox"/> each 6 months <input type="checkbox"/> each year <input type="checkbox"/> each [] year(s) <input checked="" type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment
---------------------	---

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: <input checked="" type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: <input type="checkbox"/> racial or ethnic origin <input type="checkbox"/> political opinions <input type="checkbox"/> religious or philosophical beliefs <input type="checkbox"/> trade union membership <input type="checkbox"/> genetic data <input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> physical or mental health <input type="checkbox"/> sex life or sexual orientation <input type="checkbox"/> criminal convictions and offences <input checked="" type="checkbox"/> none of the above* * For additional clarity, Customer agrees that it will not make available the following categories of information to LogiSense: government issued personal identification numbers, consumer financial account information,

	<p>credit and payment card information, personal health information, or information deemed “sensitive” under applicable Data Protection Law (such as racial or ethnic origin, political opinions, or religious or philosophical beliefs) except with LogiSense’s prior written approval. For the purpose of clarity examples of government issued personal identification numbers are drivers’ license numbers, Social Security Numbers (U.S)/ Social Insurance Number (Canada) or the equivalent in the European Union, passport numbers, etc., but not information that is typically included in billing systems such as taxation numbers, company numbers, address, etc.</p> <p><input type="checkbox"/> set out in:</p> <p>And:</p> <p><input type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
<p>Relevant Subjects</p>	<p>Data</p> <p>The Data Subjects of the Transferred Data are:</p> <p><input checked="" type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
<p>Purpose</p>	<p><input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes:</p> <p><input type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in: the Linked Agreement</p> <p>In both cases, any other purposes which are compatible with the purposes set out above.</p> <p><input checked="" type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>

Table 4: Security Requirements

Security Transmission of	Please see Annex I
Security of Storage	Please see Annex I
Security Processing of	Please see Annex I
Organisational security measures	Please see Annex I
Technical security minimum requirements	Please see Annex I
Updates to the Security Requirements	<input checked="" type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	
(iii) Extra contractual protections	

Part 3: Commercial Clauses

Commercial Clauses	N/A
---------------------------	-----

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

- 1.2.2 Part two: Extra Protection Clauses;
 - 1.2.3 Part three: Commercial Clauses; and
 - 1.2.4 Part four: Mandatory Clauses.
- 1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
- 1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
- 1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.
- 2. Legal Meaning of Words**
- 2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
- 2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.
- 3. You have provided all the information required**
- 3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
- 3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
- 3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
 - 3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.
- 3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.
- 4. How to sign the IDTA**
- 4.1 The Parties may choose to each sign (or execute):
- 4.1.1 the same copy of this IDTA;
 - 4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

- 4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

- 5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

- 5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;
- 5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;
- 5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or
- 5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

- 5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.4 From time to time, the ICO may publish a revised Approved IDTA which:

- 5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or
- 5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

- 6.1 This IDTA 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.
- 6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.
- 6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.
- 6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.
- 6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.
- 6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.
- 6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):
 - 6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and
 - 6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.
- 6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.
- 6.9 References to:

- 6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;
- 6.9.2 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 IDTA has been signed; and
- 6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

- 7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

- 8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
 - 8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
 - 8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
- 8.2 The Exporter must:
 - 8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and
 - 8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.
- 8.3 The Importer must:
 - 8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");
 - 8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

- 8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and
 - 8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.
- 8.4 The Importer must ensure that at the Start Date and during the Term:
- 8.4.1 the Importer Information is accurate;
 - 8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.
- 8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
- 9. Reviews to ensure the Appropriate Safeguards continue**
- 9.1 Each Party must:
- 9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and
 - 9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.
- 9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
- 9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;
 - 9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

12.1 The Importer must:

- 12.1.1 only Process the Transferred Data for the Purpose;
 - 12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
 - 12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
 - 12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
 - 12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and
 - 12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).
- 12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.
- 13. Importer's obligations if it is subject to the UK Data Protection Laws**
- 13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:
- 13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and
 - 13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.
- 13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:
- Section 14 (Importer's obligations to comply with key data protection principles);
 - Section 15 (What happens if there is an Importer Personal Data Breach);
 - Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
 - Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).
- 14. Importer's obligations to comply with key data protection principles**
- 14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.
- 14.2 The Importer must:

- 14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;
 - 14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and
 - 14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.
- 15. What happens if there is an Importer Personal Data Breach**
- 15.1 If there is an Importer Personal Data Breach, the Importer must:
 - 15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and
 - 15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
 - 15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:
 - 15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
 - 15.2.1.1 a description of the nature of the Importer Personal Data Breach;
 - 15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
 - 15.2.1.3 likely consequences of the Importer Personal Data Breach;
 - 15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
 - 15.2.1.5 contact point for more information; and
 - 15.2.1.6 any other information reasonably requested by the Exporter,
 - 15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

- 15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.
- 15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
- 15.3.1 a description of the nature of the Importer Personal Data Breach;
 - 15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
 - 15.3.3 likely consequences of the Importer Personal Data Breach;
 - 15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
 - 15.3.5 contact point for more information; and
 - 15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

- 15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.
- 15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

- 16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:
- 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based

on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

- 16.1.2 the third party has been added to this IDTA as a Party; or
 - 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
 - 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
 - 16.1.5 the transfer is to the UK or an Adequate Country.
- 16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).
- 17. Importer's responsibility if it authorises others to perform its obligations**
- 17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
- 17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.
- 17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.
- 17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

- 18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:
- 18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;
 - 18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;
 - 18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand

the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

- 20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and
 - 20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.
- 20.5 If a Relevant Data Subject requests, the Importer must:
- 20.5.1 rectify inaccurate or incomplete Transferred Data;
 - 20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;
 - 20.5.3 cease using it for direct marketing purposes; and
 - 20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.
- 20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the “Decision-Making”), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:
- 20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or
 - 20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or
 - 20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.
- 21. How Relevant Data Subjects can exercise their data subject rights- if the Importer is the Exporter’s Processor or Sub-Processor**
- 21.1 Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.
- 22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws**
- 22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:
- 22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

- 22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or
- 22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access

- 23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.
- 23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.
- 23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.
- 23.4 In so far as Local Laws allow, the Importer must:
 - 23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and
 - 23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

- 24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.
- 24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.
- 24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

- 26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.
- 26.2 In this IDTA “Significant Harmful Impact” means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.
- 27. Breaches of this IDTA by the Importer**
- 27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:
- 27.2.1 the Exporter must suspend sending Transferred Data to the Importer;
- 27.2.2 If the Importer is the Exporter’s Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and
- 27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:
- 27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and
- 27.2.3.2 if the third party receiver is the Importer’s Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).
- 27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.
- 28. Breaches of this IDTA by the Exporter**
- 28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.
- 28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

- 29.1.1 at the end of the Term stated in Table 2: Transfer Details; or
- 29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;
- 29.1.3 at any time that the Parties agree in writing that it will end; or
- 29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 “Ending the IDTA when the Approved IDTA changes”, will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

- 29.2.1 its direct costs of performing its obligations under the IDTA; and/or
- 29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA 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 IDTA.

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

- 30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and
 - 30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or
 - 30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;
- 30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

- 31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;
 - 31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and
 - 31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.
- 31.2 When this IDTA ends (no matter what the reason is):
- 31.2.1 the Exporter must stop sending Transferred Data to the Importer; and
 - 31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;
 - 31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.
 - 31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):
 - Section 1 (This IDTA and Linked Agreements);
 - Section 2 (Legal Meaning of Words);
 - Section 6 (Understanding this IDTA);
 - Section 7 (Which laws apply to this IDTA);
 - Section 10 (The ICO);
 - Sections 11.1 and 11.4 (Exporter's obligations);
 - Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
 - Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
 - Section 17 (Importer's responsibility if it authorised others to perform its obligations);
 - Section 24 (Giving notice);
 - Section 25 (General clauses);
 - Section 31 (What must the Parties do when the IDTA ends);
 - Section 32 (Your liability);
 - Section 33 (How Relevant Data Subjects and the ICO may bring legal claims);

- Section 34 (Courts legal claims can be brought in);
- Section 35 (Arbitration); and
- Section 36 (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, “Party One”) agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One’s breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One’s breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One’s Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party’s responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- Section 1 (This IDTA and Linked Agreements);
- Section 3 (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- Section 8 (The Appropriate Safeguards);
- Section 9 (Reviews to ensure the Appropriate Safeguards continue);
- Section 11 (Exporter’s obligations);

- Section 12 (General Importer Obligations);
- Section 13 (Importer's obligations if it is subject to UK Data Protection Laws);
- Section 14 (Importer's obligations to comply with key data protection laws);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 16 (Transferring on the Transferred Data);
- Section 17 (Importer's responsibility if it authorises others to perform its obligations);
- Section 18 (The right to a copy of the IDTA);
- Section 19 (The Importer's contact details for the Relevant Data Subjects);
- Section 20 (How Relevant Data Subjects can exercise their data subject rights);
- Section 21 (How Relevant Data Subjects can exercise their data subject rights- if the Importer is the Exporter's Processor or Sub-Processor);
- Section 23 (Access Requests and Direct Access);
- Section 26 (Breaches of this IDTA);
- Section 27 (Breaches of this IDTA by the Importer);
- Section 28 (Breaches of this IDTA by the Exporter);
- Section 30 (How to end this IDTA if there is a breach);
- Section 31 (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

- 34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).
- 34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
- 34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

- 35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.
- 35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.
- 35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.
- 35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.
- 35.5 The English language must be used in the arbitral proceedings.
- 35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: <ul style="list-style-type: none"> • a territory; • one or more sectors or organisations within a third country; • an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's 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 IDTA	The template IDTA A1.0 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 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Data Category	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
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.
Without Undue Delay	Without undue delay, as that phrase is interpreted in the UK GDPR.

Annex I

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer has a thorough suite of information security policies that are based on the SSAE18, PCIDSS information security standards and GDPR, and include policies related to:

Acceptable Use

Access Control

Change Management

Endpoint Security

Information Classification

Human Resource Security

Logging and Monitoring

Operations Backup

Password

Physical and Environment Security

Security Incident Management

Security Risk Management

Security Vulnerability Management

Third-Party Risk Management

Wireless Security

The foundation of these policies is the principle that data is accessed only as required and they are anchored in the key concepts of least-privilege, need-to-know, and segregation of duties. Data importer reviews these policies annually or as required, including upon the occurrence of a significant change to its business process or environment, or to applicable legislation.

Verification of Security Controls

Data importer performs internal testing of key security and privacy controls to verify its compliance with established internal frameworks, including third party security penetration testing on an annual basis. The results of this internal testing are then shared with executive management as applicable; any required substantive remediation efforts are then monitored and controls are re-tested, as required, to ensure compliance with established internal frameworks.



On an semi-annual basis, an independent third party audits data importer's security and privacy controls to verify that the required technology, processes and procedures are in place, and that such processes and procedures are being followed.

A summary of our SOC 1 Type II report may be requested through your account manager.

Annex II

List of Sub-Processors to Whom Importer MAY Transfer on the Transferred Data

Sub-Processor	Purpose	Country	DPA Reference
Amazon Web Services Inc.	Applicaiton Cloud infrastructure	USA	https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/#:~:text=Data%20Processing%20Addendum(.pdf
Spreadly	Payment Processing and Gateway Integration	USA	https://www.spreadly.com/gdpr#:~:text=of%20which%20is-,hosted%20here.,-This%20DPA%20provides
Workato	Workflow and Integration Automation	USA	https://www.workato.com/legal/dpa
Critical River	Implementation and Onboarding Services	USA	
Anita Middleton LLC	Technical Support services for the platform	USA	