DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of the Distribution and Representation Agreement (the "Agreement") between

Delta Intelligent Building Technologies (Canada) Inc., having its corporate office located at 17850 56 Ave, Surrey, BC V3S 1C7, Canada ("**Data Controller**")

and

COMPANY, and its affiliated companies, having its office located at ADDRESS ("**Data Processor**")

Together hereinafter referred to as the "Parties".

1. DEFINITIONS

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. Seq, and its implementing regulations, as may be amended from time to time.

"Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

"Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, Canada, United States and other jurisdictions applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the individual to whom Personal Data relates.

"Personal Data" means any information relating to an identified or identifiable person. The types of Personal Data Processed under this DPA include but are not limited to the following: name, business contact information including but not limited to address, phone number, email, job title, company, location.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

"Security Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Personal Data transmitted, stored or otherwise Processed on the Data Processor's equipment or facilities.

"Sub-processor" means any sub-contractor engaged by the Data Processor that will Process Personal Data on behalf of the Data Controller through the Data Processor.

2. PROCESSING OF PERSONAL DATA

2.1. The Data Processor shall Process Personal Data provided by the Data Controller in accordance with the requirements of the Data Protection Laws and the Data Processor will ensure that the instructions for the Processing of Personal Data shall comply with the Data Protection Laws, based on the training provided by the Data Controller as a requirement for the Data Processor to Process Personal Data. If the Data Processor believes or becomes aware that any of the Data Controller's instructions conflicts with any Data Protection Laws, the Data Processor shall inform the Data Controller.

2.2. During the term of the Agreement, the Data Processor shall only Process Personal Data on behalf of and in accordance with the Agreement and Data Controller's instructions, except as required to comply with a legal obligation to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless the law explicitly prohibits the furnishing of such information to the Data Controller. The Data Processor shall never process the Personal Data in a manner inconsistent with the Data Controller's documented instructions.

2.3. The Data Processor acknowledges and confirms that it shall not have, derive, or exercise any rights or benefits regarding Personal Data Processed on the Data Controller's behalf, nor shall it combine the Personal Data Processed on the Data Controller's behalf with any information it processes on behalf of any other parties, and may use and disclose Personal Data solely for the purposes for which such Personal Data was provided to it, as stipulated in the Agreement and this DPA. The Data Processor certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling and/or sharing (as such terms are defined in the CCPA) any Personal Data Processed hereunder without the Data Controller's prior written consent, not taking any action that would cause any transfer of Personal Data to or from the Data Processor under the Subscription Service or this DPA to qualify as "selling" or "sharing" such Personal Data under the CCPA.

3. CONFIDENTIALITY

3.1. Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. SECURITY

4.1. The Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

(a) measures to ensure that the Personal Data can be accessed only by authorized personnel;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and flexibility of processing systems and services;
(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data;
(e) measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller.

4.2. At the request of the Data Controller, the Data Processor, shall demonstrate the measures it has taken pursuant to this Article 4 and shall allow the Data Controller to audit and test such measures. The Data Controller shall be entitled to giving at least 30 days' notice to the Data Processor to carry out or have carried out by a third party who has entered into a confidentiality agreement with the Data Processor, audits of the Data Processor's premises and operations as these relate to the Personal Data. The Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller and shall grant the Data Controller's auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Data Processor shall provide the Data Controller and/or the Data Controller's auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Data Controller to ascertain the Data Processor’s compliance with this Data Processing Agreement.

5. CONTRACTING WITH SUB-PROCESSORS

5.1. The Data Processor shall not subcontract any of its service-related activities consisting of the Processing of the Personal Data or requiring Personal Data to be Processed by any third party without the prior written authorization of the Data Controller.

5.2. Notwithstanding any authorization by the Data Controller within the meaning of the preceding paragraph, the Data Processor shall remain fully liable, including but not limited to indemnifying against any third party damages alleged against Data Controller, in relation to the Data Controller for any actions of any such sub-processor that fails to fulfil its data protection obligations or causes any other damage to Data Controller.

5.3. The Data Processor shall ensure that any sub-processor is bound by the same data protection obligations of the Data Processor under this Data Processing Agreement, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Laws.

6. ASSISTANCE TO DATA CONTROLLER

6.1. The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subjects' rights under the Data Protection Laws, including GDPR.

6.2. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of Processing and the information available to the Data Processor.

6.3. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

6.4. The Data Processor shall assist the Data Controller with any prior consultations, correspondence, enquiries and/or complaints from supervisory authorities in connection with the Processing subject to this Subscription Service. In the event that any such correspondence, enquiry or complaint is made directly to the Data Processor, the Data Processor shall promptly inform the Data Controller providing full details of the same.

6.5. If the Data Processor believes or becomes aware that its Processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform the Data Controller and provide the Data Controller with all such reasonable and timely assistance as the Data Controller may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant supervisory authority.

6.6. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations under the Data Protection Laws.

7. INFORMATION OBLIGATIONS AND SECURITY BREACH MANAGEMENT

7.1. When the Data Processor becomes aware of a Security Breach that impacts the Processing of the Personal Data that is the subject of the Agreement, it shall promptly notify the Data Controller about the Security Breach, shall at all times cooperate with the Data Controller, and shall follow the Data Controller's instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the Security Breach, to formulate a correct response, and to take suitable further steps in respect of the Security Breach.

7.2. The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about a Security Breach.

Where the Security Breach is reasonably likely to require a data breach notification by the Data Controller under applicable Data Protection Laws, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller no later than 24 hours of having become aware of such a Security Breach.

7.3. Any notifications made to the Data Controller pursuant to a Security Breach will be delivered to one or more of the Data Controller's business, technical or administrative contacts by means of email and shall contain:

(a) a description of the nature of the Security Breach, including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
(b) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;
(c) a description of the likely consequences of the Security Breach; and
(d) a description of the measures taken or proposed to be taken by the Data Processor to address the Security Breach including, where appropriate, measures to mitigate its possible adverse effects.

8. RETURNING OR DESTRUCTION OF PERSONAL DATA

8.1. Upon termination of this Data Processing Agreement, upon the Data Controller's written request, or upon fulfillment of all purposes agreed in the context of the Agreement whereby no further processing is required, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies.

8.2. The Data Processor shall notify all third parties supporting its own processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

9. LIABILITY AND INDEMNITY

9.1. The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Controller and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Data Protection Laws by the Data Processor.

10. DURATION AND TERMINATION

10.1. This Data Processing Agreement shall come into effect on <DATE>.

10.2. Termination or expiration of this Data Processing Agreement shall not

discharge the Data Processor from its confidentiality obligations pursuant to Article 3.

10.3. The Data Processor shall process Personal Data until the date of termination of this Agreement, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on instruction of the Data Controller.

_____

On behalf of the Company

_____

Date

_____

On behalf of Delta Intelligent Building Technologies (Canada) Inc.

_____

Date