Schedule 5

Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the agreement between Vendor (as defined below) and Customer (as defined below) for the services provided by Vendor to Customer (collectively, the "**Agreement**"). For the purposes of this DPA, "**Customer**" means the entity set forth in the Project Order to which this DPA is incorporated by reference (the "**Project Order**") and "**Vendor**" means BiltOn Technologies Inc.

This DPA describes the commitments of Customer and the Vendor (each a "**Party**" and together, the **"Parties"**) concerning the processing of Personal Data in connection with the provision of one or more services (the "**Services**") contemplated by the Agreement.

The terms used in this DPA have the meaning set forth in this DPA. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement.

The Parties agree as follows:

Definitions. The following capitalized terms, when used in this DPA, will have the corresponding meanings provided below:

1.1 "**Applicable Data Protection Laws**" means all worldwide privacy and data protection laws, regulations, rules, ordinances and other decrees applicable to the Personal Data, including (but not limited to): (i) European Data Protection Laws; and (iii) US Privacy Laws; as may be amended, superseded or replaced.

1.2 "**EEA**" means the countries that are parties to the agreement on the European Economic Area and Switzerland.

1.3 "**Customer Personal Data"** means any Personal Data processed by Vendor on behalf of Customer as a service provider or processor (as applicable) in connection with the Agreement, as more particularly described in Annex I of this DPA**.**

1.4 **"European Data Protection Laws"** means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC ("**e-Privacy Directive**"); (iii) any applicable national implementations of (i) and (ii); (iv) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance ("**Swiss DPA**"); and (v) in respect of the United Kingdom ("**UK**"), the Data Protection Act 2018 and the GDPR as saved into UK law by virtue of section 3 of the UK's European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to have effect by virtue of section 2 of the UK's European Union (Withdrawal) Act 2018; in each case as may be amended, superseded or replaced.

1.5 "**Personal Data**" means any information that relates to an identified or identifiable natural person and which is protected as "personal data," "personal information," or "personally identifiable information" under Applicable Data Protection Laws.

1.6 "**Restricted Transfers**" means: (i) where the GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission (an "**EEA Restricted Transfer**"); (ii) where the UK GDPR applies, a

transfer of Personal Data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018 (a "**UK Restricted Transfer**"); and (iii) where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

1.7 **"Security Incident"** means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data transmitted, stored or otherwise processed by Vendor and/or its Sub-processors in connection with the provision of the Services.

1.8 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses adopted by the EU Commission by means of the Implementing Decision EU 2021/914 of June 4, 2021.

1.9 **"Sub-processor"** means any processor engaged by Vendor or its Affiliates to assist in fulfilling its obligations with respect to providing the services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Vendor affiliates.

1.10 "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by UK Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018.

1.11 **"US Privacy Laws**" means, as applicable: the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq. (2018) as amended by the California Privacy Rights Act of 2020 ("**CPRA**") (together the "**CCPA**"), the Virginia Consumer Data Protection Act ("**VCDPA**"), as of July 1, 2023, the Connecticut Data Privacy Act ("**CTDPA**"), the Colorado Privacy Act ("**CPA**"), and as of December 31, 2023, the Utah Consumer Privacy Act ("**UCPA**"), and all US privacy laws that may come into effect from time to time.

1.12 The terms **"controller", "processor"** and "**processing"** shall have the meanings given to them in the applicable European Data Protection Laws, and **"process", "processes"** and **"processed"** shall be interpreted accordingly; and the terms **"business", "business purpose", "consumer", commercial purpose", "personal information", "service provider"**, **"sell" and "share"** shall have the meanings given to them in applicable US Privacy Laws**.**

Role and Scope of Processing

2.1 **Scope.** This DPA applies to the extent that Vendor processes any Customer Personal Data as a processor or service provider (as applicable).

2.2 **Role of the Parties.** The Parties acknowledge and agree that Customer is a controller with respect to the processing of Customer Personal Data, and Vendor shall process Customer Personal Data only as a processor on behalf of Customer, as further described in Annex I of this DPA. Any processing by either Party of Customer Personal Data under or in connection with the Agreement shall be performed in accordance with Applicable Data Protection Laws.

2.3 **Vendor processing of Personal Data.** Vendor agrees that it shall process Customer Personal Data only for the purposes described in the Agreement and in accordance with Customer's documented lawful instructions. The Parties agree that the Agreement and this DPA set out Customer's complete and final instructions to Vendor in relation to the processing of Customer Personal Data. Vendor shall notify Customer in writing, unless prohibited from doing so under Applicable Data Protection Laws, if it becomes aware or believes that any data processing instructions from Customer violates Applicable Data Protection Laws. Notwithstanding anything to the contrary in the Agreement, Vendor shall not process Customer Personal Data for its own internal purposes including but not limited to in an anonymized or aggregated form.

Sub-processing

3.1 **Authorized Sub-processors.** Customer acknowledges and agrees that Vendor may engage Sub-processors to process Customer Personal Data on Customer's behalf, provided that Customer

approves each such Sub-processor. The Sub-processors currently engaged by Vendor and authorized by Customer are attached as Annex III. Vendor shall notify Customer in writing if it changes its Sub-processors at least 30 days in advance to any such changes.

3.2 **Objections to Sub-processors**. Customer may object in writing to Vendor's appointment of a new Sub-processor by notifying Vendor promptly in writing within thirty (30) calendar days of receipt of Vendor notice in accordance with Section 3.1 above. Such notice shall explain the reasonable grounds for the objection and the Parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Vendor will, at its sole discretion, either not appoint Sub-processor, or permit Customer to suspend or terminate the affected service in accordance with the termination provisions in the Agreement without liability to either Party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

3.3 **Sub-processor Obligations**. Vendor shall: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Personal Data to the standard required by Applicable Data Protection Laws and this DPA; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Vendor to breach any of its obligations under this DPA.

Security and Audits

4.1 **Vendor Security Measures**. Vendor shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data ("**Security Measures**"). Such measures will include, at a minimum, those measures described in Annex II of this DPA. Vendor shall ensure that any person who is authorized by Vendor to process Customer Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.2 **Security Incident Response**. Upon becoming aware of a Security Incident, Vendor shall notify Customer without undue delay and shall: (i) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (ii) promptly take steps, necessary to contain, investigate, and remediate any Security Incident.

4.3 **Audits**. Vendor shall supply a copy of any audit reports, such as a Service Organization Control (SOC) 2 and/or ISO 27001 or a comparable report ("**Reports**"), to Customer, so that Customer can verify Vendor's compliance with this DPA. In addition to the Reports, Vendor shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its processing of Customer Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Vendor's compliance with this DPA, provided that Customer shall not exercise this right more than once in any 12 month rolling period. In addition, Customer may also conduct an audit of Vendor's data protection compliance program and compliance with this DPA if (i) the above measures are not sufficient to confirm compliance with this DPA or reveal some material issues, (ii) Customer is expressly requested or required by a data protection authority to conduct such an audit, or (iii) Vendor has experienced a Security Incident.

4.4 **Vendor Data Protection Measures**. In addition to the Security Measures described herein, Vendor shall implement appropriate technical and organizational measures to ensure data protection for the Customer Personal Data, including but not limited to: (i) measures for certification or similar assurance of data protection in processes and products; (ii) measures for ensuring data minimization; (iii) measures for ensuring data quality; (iv) measures for ensuring limited data retention; (v) measures for ensuring accountability; (vi) measures for allowing data portability where required by Applicable Data Protection Law; and (vii) measures for ensuring erasure.

International Transfers

5.1 **Processing locations.** Customer acknowledges and agrees that Vendor may transfer and process Customer Personal Data to and in the locations where Vendor, its Affiliates or its Sub-processors maintain data processing operations. Vendor shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this DPA.

Deletion of Customer Personal Data

6.1 Upon termination or expiry of the Agreement, Vendor shall delete all Customer Personal Data (including copies) in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent Vendor is required by applicable law to retain some or all of the Customer Personal Data, in which case Vendor shall retain such Customer Personal Data in compliance with all Applicable Data Protection Laws.

Rights of Individuals and Cooperation

7.1 **Data Subject Requests.** To the extent that Customer is unable to independently access the relevant Customer Personal Data, Vendor shall, taking into account the nature of the processing, provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Personal Data under the Agreement. In the event that any such request is made to Vendor directly, Vendor shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Vendor is required to respond to such a request, Vendor shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

7.2 **Subpoenas and Court Orders**. If a law enforcement agency sends Vendor a demand for Customer Personal Data (for example, through a subpoena or court order), Vendor shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Vendor is legally prohibited from doing so in which case Vendor shall take all reasonable steps to challenge such prohibition.

Jurisdiction Specific Terms

8.1 **EEA and UK.** To the extent the Customer Personal Data is subject to European Data Protection Laws, the following terms shall apply in addition to the terms in the remainder of this DPA:

(a) Data Protection Impact Assessment. To the extent Customer is required under applicable European Data Protection Law, Vendor shall provide reasonably requested information regarding Vendor processing of Personal Data under the Agreement to enable Customer to carry out data protection impact assessments or prior consultations with supervisory authorities as required by law.

8.2 **Restricted Transfers.**

8.2.1 **GDPR**. To the extent any transfer of Customer Personal Data to Vendor from Customer is a Restricted Transfer, Vendor agrees to abide by and process Customer Personal Data in compliance with the Standard Contractual Clauses, which shall be deemed incorporated into this DPA as follows:

(a) Customer is the controller of the Customer Personal Data and Vendor is the processor. Module Two (*controller to processor transfers*) shall apply;

(b) In Clause 7, the optional docking clause will apply;

(c) In Clause 9, Option 2 will apply and the time period for prior notice of Sub-processor changes shall be as set out in Section 3.1 of this DPA;

(d) In Clause 11, the optional language will not apply;

(e) In Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by the law of Ireland;

(f) In Clause 18(b), disputes shall be resolved before the courts of Ireland; and

(g) Annex I and II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annexes I and II to this DPA;

8.2.2 **UK GDPR**. To the extent any transfer of Customer Personal Data to Vendor from Customer is a Restricted Transfer to which the UK GDPR applies, the Standard Contractual Clauses shall apply in accordance with Section 8.2.1 above, but as modified and interpreted by the Part 2: Mandatory Clauses of the UK Addendum, which shall be incorporated into and form an integral part of this DPA. Any conflict between the terms of the Standard Contractual Clauses and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex I and Annex II to the Standard Contractual Clauses, attached to this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

8.2.3 **Swiss DPA**. To the extent any transfer of Customer Personal Data to Vendor from Customer is a Restricted Transfer to which the Swiss DPA applies, the Standard Contractual Clauses shall apply in accordance with Section 8.2.1 above, but with the following modifications:

(a) any references in the Standard Contractual Clauses to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein;

(b) any references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be;

(c) any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland; and

(d) the Standard Contractual Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

8.3 **US Privacy Laws.** To the extent the Customer Personal Data is subject to US Privacy Laws, the Parties agrees that Customer is a business and that it appoints Vendor as its service provider or processor to process Customer Personal Data for the limited and specific business purpose as permitted under the Agreement (including this DPA) and US Privacy Laws, or for purposes otherwise agreed in writing (the "**Permitted Purposes**"). Customer and Vendor further agree that:

(a) Vendor shall not retain, use or disclose personal information for any purpose other than the Permitted Purposes; including retaining, using or disclosing personal information for a commercial purpose other than the Permitted Purposes;

(b) Customer is not sharing or selling personal information to Vendor and Vendor shall not sell or share personal information; and

(c) Vendor shall not retain, use or disclose personal information outside of the direct business relationship between Customer and Vendor;

(d) Vendor shall comply with its applicable obligations under US Privacy Laws and shall provide the same level of privacy protection as is required by US Privacy Laws;

(e) Customer has the right to take reasonable and appropriate steps to help ensure Vendor processes the personal information in a manner consistent with Customer's obligations under US Privacy Laws;

(f) Vendor shall immediately notify Customer if it decides it can no longer meet its obligations under US Privacy Laws;

(g) Customer shall have the right, upon notice, including under the previous Section 8.3(f), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information;

(h) If Vendor engages other service providers to assist in the processing of personal information for the Permitted Purposes under the Agreement on behalf of Customer in accordance with this DPA, such engagements must be pursuant to a written contract(s) binding such additional service providers to observe all applicable requirements of US Privacy Laws;

(i) Vendor shall not combine the personal information which Vendor receives from or on behalf of Customer, with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer;

(j) Customer is permitted to monitor Vendor's compliance with the Agreement through measures, including, but not limited to, ongoing manual reviews and regular assessments, audits, or other technical and operational testing at least once every 12 months, in accordance with Section 4.3 of this DPA;

(k) Vendor shall, taking into account the nature of the processing, reasonably cooperate with Customer in responding to verifiable consumer requests, including deleting personal information or enabling the business to do so, and notifying its own service providers or contractors to delete the personal information; and

(l) Vendor certifies that it understands the restrictions set out in this Section 8.3 and will comply with them.

Miscellaneous

9.1 Except for the changes made by this DPA as applicable to the Agreement, the Agreement remains unchanged and in full force and effect; provided however that any limitations on liability and/or disclaimers of damages contained in the Agreement shall not apply to any damages arising from Vendor's breach of this DPA.

9.2 The Parties acknowledge and agree that, by executing the Agreement, Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Affiliates (as defined in the underlying Agreement), thereby establishing a separate DPA between Vendor and each such Affiliate subject to the provisions of the Agreement and this Section. For the avoidance of doubt, an Affiliate is not and does not become a party to the Agreement, but is only a party to this DPA. Customer shall remain responsible for coordinating all communication with Vendor under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates.

9.3 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

The Parties consent to the terms of this DPA via the execution of the initial Project Order.

ANNEX I

A. LIST OF PARTIES

Processor (importer)

1. Name: BiltOn Technologies Inc.

Address: 25 Kent Ave., Brooklyn, NY, 11249

Contact person's name, position and contact details: support-US@bilton.tech

Activities relevant to the data transferred under these Clauses: BiltOn receives data collected by Customer directly to BiltOn's platform to: (a) provide the Platform to Customer and its Authorized Users and to provide the Professional Services and Support and Maintenance; (b) to improve the Platform, the Professional Services or the Support and Maintenance; (c) for all internal purposes; and (d) as otherwise permitted by the Agreement or an applicable Project Order.

Role: Processor/Sub-processor

Controller (exporter)

1. Name: As set forth in the Project Order

Address: As set forth in the Project Order

Contact person's name, position and contact details: As set forth in the Project Order

Activities relevant to the data transferred under these Clauses: Customer grants BiltOn a license to access, receive, download (as applicable), store, reproduce, distribute, modify and otherwise use the Customer Data to: (a) provide the Platform to Customer and its Authorized Users and to provide the Professional Services and Support and Maintenance; (b) to improve the Platform, the Professional Services or the Support and Maintenance; (c) for all internal purposes; and (d) as otherwise permitted by the Agreement or an applicable Project Order.

Role: Controller (and where BiltOn is the Subprocessor, then Processor)

B. DESCRIPTION OF TRANSFER

- **Categories of data subjects whose personal data is transferred**

Customer Personal Data transferred to BiltOn under the Agreement may concern the following categories of data subjects: individuals (including without limitation Customer's employees, consultants and subcontractors) whose personal data or personal information is provided by Customer for processing by BiltOn in order to provide the Platform and perform all other Professional Services and support as set forth in the Agreement.

- **Categories of personal data transferred**

Customer Personal Data transferred concern the following categories of data (please specify):

- Business contact information of Company (name and business e-mail address) in all cases.
- Name of employees, subcontractors, identifying number, email address, telephone,

- **Sensitive data transferred**

Biometric information (photo)

Where sensitive data is transferred, the following restrictions or safeguards are applied: strict purpose limitation, access restrictions (including access only for staff having been specifically trained), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- **Frequency of the transfer**

data transferred upon onboarding and may be updated

- **Nature of the processing**

Company personal data transferred to BiltOn to provide Platform and carryout Professional Services and support as set forth in the Agreement.

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

The operation, support, or use of the Platform as set out in the Agreement, including to improve the Platform, provide Professional Services and support and as otherwise permitted in the Project Order and in compliance with applicable laws.

- **The period for which the personal data will be retained**

The duration of the processing under this DPA is until the termination of the applicable subscription and as permitted by applicable law.

C. COMPETENT SUPERVISORY AUTHORITY

To the extent applicable, in the event that personal data of data subjects who are subject to the GDPR is collected, then in Ireland.

ANNEX II

Security Measures

Description of the technical and organizational security measures implemented by the data processor/importer in accordance with the Standard Contractual Clauses. The data processor will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data provided by the data exporter in fulfilment of the services, including the following:

1. **Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed. These measures include:

- Establishing security areas, restriction of access paths
- Establishing access authorizations for employees and third parties
- Access control system (magnetic card, chip card)
- Key management, card-keys procedures
- Door locking (electric door openers etc.)
- Surveillance facilities, video/CCTV monitor, alarm system
- Securing decentralized data processing equipment and personal computers
- Additional measures as necessary to ensure the physical security of locations where personal data is processed

2. **Virtual access control**

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons. These measures include:

- User identification and authentication procedures
- ID/password security procedures (special characters, minimum length, change of password)
- Automatic blocking (e.g. password or timeout)
- Creation of one master record per user, user master data procedures,
- Encryption of archived data media
- Endpoint protection on workstations

3. **Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization. These measures include:

- Internal policies and procedures
- Control authorization schemes
- Differentiated access rights (profiles, roles, transactions and objects)
- Monitoring and logging of accesses
- Disciplinary action against employees who access Personal Data without authorization
- Reports of access
- Access procedure
- Change procedure
- Deletion procedure
- Encryption

4. **Disclosure control**

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed. These measures include:

- Encryption/tunneling
- Logging
- Transport security

5. **Entry control**

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems. These measures include:

- Logging and reporting systems
- Audit trails and documentation

6. **Control of instructions**

Technical and organizational measures ensuring Personal Data are processed solely in accordance with the Instructions of the Controller. These measures include:

- Unambiguous wording of the contract
- Formal commissioning (request form)
- Criteria for selecting the Processor

7. **Availability control**

Technical and organizational measures ensuring Personal Data are protected against accidental destruction or loss (physical/logical). These measures include:

- Backup procedures
- Cloud Storage redundancy and availability
- Uninterruptible power supply (UPS)
- Remote storage of backups
- Anti-virus/firewall systems
- Disaster recovery plan

8. **Separation control**

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately. These measures include:

- Separation of databases
- Segregation of functions (production/testing)
- Procedures for storage, amendment, deletion, transmission of data for different purposes

ANNEX III

List of Sub-Processors

The controller has authorized the use of the following Sub-processors:

Name: AWS

Address: North Virginia (US East 1)

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Cloud Storage Services