DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) is entered into by and between the entity accepting this DPA (“Customer”) and Brizo Data Inc. ("Brizo"). This DPA is supplemental to the Brizo Master Agreement Terms and Conditions entered into between the parties which governs the provision of the Brizo services provided by Brizo to Customer ("Agreement").

1. DEFINITIONS

1.1 Definitions: In this DPA, the following terms shall have the following meanings:

(a) "Applicable Data Protection Law" means all privacy and data protection laws that apply to Brizo’s processing of Data under the Agreement (including, where applicable, any applicable Canadian federal and provincial laws, California Consumer Privacy Act of 2018 including its associated regulations and as amended (the "CCPA"), and European Data Protection Law).

(b) Controller" means the entity that determines the purposes and means of the processing of Personal Data;

(c) "Data" means Personal Data provided by Customer (directly or indirectly) to Brizo for processing under the Agreement as more particularly identified in Appendix A (Processing Particulars);

(d) "European Data Protection Law" means all EU and U.K. regulations or other legislation applicable (in whole or in part) to the processing of Personal Data under the Agreement (such as Regulation (EU) 2016/679 (the "GDPR"), the U.K. GDPR (defined below), and the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss Addendum"); the national laws of each EEA member state and the U.K. implementing any EU directive applicable (in whole or in part) to the processing of Personal Data (such as Directive 2002/58/EC); and any other national laws of each EEA member state and the U.K. applicable (in whole or in part) to the Processing of Personal Data; in each case as amended or superseded from time to time.

(e) "Model Clauses" means the standard contractual clauses attached to the European Commission's Implementing Decision of 4 June 2021 under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, on standard contractual clauses, selecting Module Two between controllers and processors in any case where Customer is a Controller, and Module Three between processors in any case where Customer is a Processor, and excluding optional clauses unless otherwise specified), and any replacement, amendment or restatement of the foregoing, as issued by the European Commission, on or after the effective date of this DPA.

(f) "Personal Data" means any information relating to an identified or identifiable natural person (a "Data Subject"), the processing of which is governed by Applicable Data Protection Law; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Where the CCPA applies, 'Personal Data' includes "personal information" as defined by the CCPA. Personal Data does not include anonymous or de-identified information or aggregated information derived from Personal Data.

(g) "Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(h) "Processor" means an entity that processes Personal Data on behalf of the Controller. Where applicable, Processor includes "service provider" as defined by the CCPA.

(i) "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data.

(j) "Sensitive Data" means any 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 or offences.

(k) "Sub-Processor" means an entity engaged by the Processor or any further sub-contractor to process Personal Data on behalf of and under the instructions of the Controller.

(l) "U.K. GDPR" means the GDPR, as it forms part of the domestic law of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018.

2. DATA PROTECTION

2.1 Relationship of the parties: As between the parties and for the purposes of this DPA, Customer appoints Brizo as a Processor to process the Data on behalf of Customer. Where applicable, Brizo is a "service provider" as defined in the CCPA. Customer shall comply with Applicable Data Protection law, including but not limited to providing notice to Data Subjects, and obtaining and periodically refreshing the consent of Data Subjects, where required, to Customer's use of Brizo's Services and Customer's own processing of Data. Customer represents and warrants it has and will continue to have the right to transfer Data to Brizo for processing in accordance with the Agreement and this DPA. Brizo shall comply with Applicable Data Protection Law and understands and shall comply with the prohibitions on Processors set forth in the CCPA with respect to such Data, including, without limitation and to the extent applicable in each case: (i) selling or sharing any Data (as the terms "sell" and "share" are each defined within the CCPA) where the sale or sharing of such Data is restricted by the CCPA, (ii) disclosing such Data to any party outside of the direct business relationship between Brizo and Customer, or (iii) retaining, using or disclosing such Data for a commercial purpose other than performing the Services as set forth in the Agreement with Customer, or as otherwise expressly permitted under this DPA or the Agreement.

2.1 Purpose limitation: Each party acknowledges and agrees that all Data is disclosed by Customer hereunder only for those limited and specified purposes set forth in the Agreement and this DPA. Brizo shall process the Data as a Processor only as necessary to perform the Services for Customer under the Agreement, and strictly in accordance with the documented instructions of Customer (including those in this DPA and the Agreement). In no event shall Brizo process the Data for its own purposes or those of any third party. Brizo may also anonymize or deidentify Data in accordance with Applicable Data Protection Law. Customer shall only give lawful instructions that comply with Applicable Data Protection Law and shall ensure that Brizo's processing of Data, when done in accordance with Customer's instructions, will not cause Brizo to violate Applicable Data Protection Law. Brizo shall inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. In any case where confirmation of a Controller's instructions is required by Applicable Data Protection Law, the parties agree that the Agreement, together with this DPA, represents the complete and final documented instructions from the Controller of the Data to Brizo as of the date of this DPA for the processing of Data. Nothing in this DPA shall be read to limit any obligations of Brizo to assist Customer with Customer's reasonable and appropriate efforts to ensure that Brizo processes such Data in a manner consistent with each party's obligations under the CCPA, including (i) the obligation to immediately notify Customer if Brizo determines it can no longer meet its obligations under the CCPA with respect to such Data, and (ii) the obligation not to combine any such Data relating to a specific consumer with any other data about the same consumer in Brizo's possession and/or control, whether received from or on behalf of another person or persons or collected by Brizo from its own interaction(s) with the consumer.

2.3 **International transfers of Data:** Brizo is located in Canada and processes the Data in Canada and United States of America. For Brizo to perform Services for Customer pursuant to the Agreement, Customer transfers (directly or indirectly) Personal Data to Brizo in the United States and Canada. For Personal Data subject to European Data Protection Law, Brizo agrees to abide by and process the Data in compliance with the Model Clauses, which are incorporated in full by reference and form an integral part of this DPA. For the purposes of the Model Clauses, the parties agree that:

2.3.1 Brizo is the "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be located outside the EEA/UK and/or a Processor acting on behalf of a third-party Controller);

2.3.2 Appendix A (Processing Particulars), Appendix B (Specific Security Measures), and Appendix C (Sub-processor List) of this DPA shall form Annex I, Annex II, and Annex III of the Model Clauses, respectively;

2.3.3 Option 2 under clause 9 of the Model Clauses will apply with respect to Sub-Processors. Annex III of the Model Clauses shall be subject to General Written Authorization, where "General Written Authorization" means that Brizo has Customer's general authorization (or the general authorization of the Controller of the Data) for the engagement of sub-processor(s) from the list set forth in Appendix C, which shall be amended from time to time in accordance with the terms of the Agreement, this DPA, and all Applicable Data Protection Law;

2.3.4 Audits described in clause 8.9 of the Model Clauses shall be carried out in accordance with the audit provisions detailed in Section 2.12 of this DPA;

2.3.5 The option under clause 11 of the Model Clauses shall not apply;

2.3.6 For purposes of clauses 17 and 18 of the Model Clauses, this DPA shall be governed by the laws of the Republic of Ireland . Any dispute arising from this DPA shall be resolved by the courts of the Republic of Ireland, and each party agrees to submit themselves to the jurisdiction of the same; and

2.3.7 It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Model Clauses. Accordingly, if and to the extent the Model Clauses conflict with any provision of this DPA, the Model Clauses shall prevail to the extent of such conflict with respect to Personal Data processed pursuant to the Model Clauses. Customer warrants it will not transfer any Sensitive Data to Brizo.

2.4 **Law enforcement requests**

2.4.1 If Brizo becomes aware that any law enforcement, regulatory, judicial or governmental authority (an "Authority") wishes to obtain access to or a copy of some or all Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Data to such Authority, Brizo shall: (a) promptly notify Customer of such Authority's data access request; (b) inform the Authority that any and all requests or demands for access to Data should be notified to or served upon Customer in writing; and (c) not provide the Authority with access to Data unless and until authorized by Customer.

2.4.2 If Brizo is under a legal prohibition that prevents it from complying with Section 2.4.1(a)-(c) in full, Brizo shall use reasonable and lawful efforts to challenge such prohibition (and Customer acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request). If Brizo makes a disclosure of

Data to an Authority (whether with Customer's authorization or due to a mandatory legal compulsion), Brizo shall only disclose such Data to the extent Brizo is legally required to do so.

2.4.3 Section 2.4.1 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Data, Brizo has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, Brizo shall notify Customer as soon as possible following such Authority's access and provide Customer with full details of the same, unless and to the extent that Brizo is legally prohibited from doing so;

2.4.4 Solely with respect to Data that is subject to the GDPR, and/or where Data whose disclosure is otherwise restricted by Applicable Data Protection Law, Brizo shall not knowingly disclose Data to an Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society. Brizo shall have in place, maintain and comply with a policy governing Personal Data access requests from Authorities which at minimum prohibits: (a) massive, disproportionate or indiscriminate disclosure of Personal Data relating to Data Subjects in the EEA and the United Kingdom; and (b) disclosure of Personal Data relating to data subjects in the EEA, and the United Kingdom to an Authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such Personal Data.

2.5 **Confidentiality of processing:** Brizo shall ensure that any person that it authorizes to process the Data (including Brizo's staff, agents and subcontractors) shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process the Data who is not under such a duty of confidentiality.

2.6 **Security:** Brizo shall implement appropriate technical and organizational measures to protect the Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data. At a minimum, such measures shall include the security measures identified in Appendix B. With respect to evaluation of the appropriate level of security for the processing of the Data, each party represents and warrants that:

2.6.1 It has taken 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; and

2.6.2 It has evaluated the use of encryption and/or pseudonymization for the Data and has determined that the level provided by Brizo is appropriate for the Data.

2.6.3 To the extent that the CCPA applies to the processing of the Data, the party has determined that the technical and organizational measures provided by Brizo is no less than the level of security required by the CCPA.

2.7 **Subcontracting:** Brizo shall not subcontract any processing of the Data to a third-party Sub-Processor unless: (i) Brizo provides to Customer an up-to-date list of its then-current Sub-Processors upon request; and (ii) Brizo provides at least thirty (30) days' prior notice of the addition or removal of any Sub-Processor (including the details of the processing it performs or will perform, and the location of such processing). If Customer objects to Brizo's appointment of a third-party Sub-Processor on reasonable grounds relating to the protection of the Data, then either Brizo will not appoint the Sub-Processor, or Customer may elect to suspend or discontinue the affected Services by providing written notice to Brizo. Customer shall notify Brizo of its objection within ten (10) business days after its receipt of Brizo's notice, and Customer's objection shall be sent to and explain the reasonable grounds for Customer's objection. If a timely objection is not made, Brizo will be deemed to have been authorized by Customer (or, if Customer is a Processor of the Data, by the Controller of the Data) to appoint

the new Sub-Processor. Brizo shall impose the same data protection terms on any Sub-Processor it appoints as those provided for by this DPA and Brizo shall remain fully liable for any breach of Brizo's obligations under this DPA that is caused by an act, error or omission of its Sub-Processor.

2.8 **Cooperation and individuals' rights:** Customer is responsible for responding to Data Subject requests using Customer's own access to the relevant Data. Brizo shall provide all reasonable and timely assistance to enable Customer to respond to: (i) any request from an individual to exercise any of its rights under Applicable Data Protection Law, and (ii) any other correspondence received from a regulator or public authority in connection with the processing of the Data. In the event that any such communication is made directly to Brizo, Brizo shall promptly (and in any event, no later than within forty-eight (48) hours of receiving such communication) inform Customer providing full details of the same and shall not respond to the communication unless specifically required by law or authorized by Customer.

2.9 **Data Protection Impact Assessment:** Taking into account the nature of the processing and the information available to Brizo, Brizo shall provide Customer with reasonable and timely assistance with any data protection impact assessments as required by Applicable Data Protection Law and, where necessary, consultations with data protection authorities.

2.10 **Security Incidents:** Upon becoming aware of a Security Incident, Brizo shall inform Customer without undue delay and shall provide all such timely information and cooperation to enable Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Brizo shall further take such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all material developments in connection with the Security Incident. Brizo shall not notify any third parties of a Security Incident affecting the Data unless and to the extent that: (a) Customer has agreed to such notification, and/or (b) notification is required to be made by Brizo under Applicable Data Protection Law.

2.11 **Deletion or return of Data:** Upon termination or expiry of the Agreement, Brizo shall (at Customer's election) delete or return all Data, including copies in Brizo's possession or control no later than within sixty (60) days of Customer's election. This requirement shall not apply to the extent that Brizo is required by applicable laws to retain some or all of the Data, in which event Brizo shall isolate and protect the Data from any further processing except to the extent required by such law, shall only retain such Data for as long as it is required under applicable laws, and shall continue to ensure compliance with all Applicable Data Protection Law during such retention.

2.12 **Audit:** Brizo uses an external auditor to verify the adequacy of its security measures and controls for its Services. Upon written request, Brizo shall provide Customer with a copy of the most recent Audit Report subject to confidentiality obligations of the Agreement or a non-disclosure agreement covering the Audit Report. If documentation beyond the Audit Report and other information that Brizo provides to Customer is necessary to enable Customer to comply with its obligations with respect to the processing of Data under Applicable Data Protection Law (such as Article 28(3)(h) of GDPR where applicable), Brizo shall permit Customer to audit Brizo's compliance with this DPA using an independent third party and shall make available all such information, systems and staff reasonably necessary to conduct such audit. Customer shall not exercise its audit rights more than once per year except following a Security Incident or following an instruction by a regulator or public authority. Customer shall give Brizo thirty (30) days prior written notice of its intention to audit, conduct its audit during normal business hours, take all reasonable measures to prevent unnecessary disruption to Brizo's operations, restrict findings to only data relevant to Customer, and provide Brizo with a copy of the auditor's report. Brizo and Customer shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to the audit. Customer shall reimburse Brizo for actual expenses and costs incurred to allow for and contribute to Customer's audit.

3. MISCELLANEOUS

3.1 The obligations placed upon the Brizo under this DPA shall survive so long as Brizo and/or its sub-Processors process Personal Data on behalf of Customer.

3.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

3.3 It is not the intention of either party, nor shall it be the effect of this DPA, to contradict or restrict any provision of the Model Clauses and/or any Applicable Data Protection Law. To the extent that any provision of the Model Clauses conflicts with this DPA, the Model Clauses shall prevail to the extent of such conflict with respect to Personal Data which is subject to the Model Clauses. In no event shall this DPA restrict or limit the rights of any Data Subject or of any Authority. If there is a change in law requiring any change to this DPA to enable either party to continue to comply with Applicable Data Protection Law, the parties will negotiate in good faith to amend this DPA to the extent reasonably necessary to comply with Applicable Data Protection Law.

3.4 If any provision of this DPA is deemed invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended to ensure its validity and enforceability while preserving the parties' intentions as closely as possible; or (ii) if that is not possible, then construed in a man-ner as if the invalid or unenforceable part had never been included herein.

3.5 The term of this DPA will terminate automatically without requiring any further action by either party upon the later of (i) the termination of the Agreement, or (ii) when all Personal Data is removed from Brizo's systems and records, and/or is otherwise rendered unavailable to Brizo for further Processing.

ANNEX A: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex A includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the processing of Customer Data

- The subject matter and duration of the processing of the Customer Data are set out in the Brizo Master Agreement and this Addendum.

The nature and purpose of the processing of Customer Data

- The nature and purpose of the processing of Customer Data are set out in the Brizo Master Agreement and this Addendum.

The types of Customer Data to be processed

- Customer may submit Personal Data, the extent of which is determined and controlled by Customer (including Customer's Users and Customers) in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

The categories of Data Subject to whom the Customer Data relates.

- Customer may submit Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

The obligations and rights of Customer

- The obligations and rights of Customer are set out in Brizo Master Agreement and this Addendum.

ANNEX B: SPECIFIC SECURITY MEASURES

Description of the technical and organizational security measures implemented by the Brizo:

Hosting and Physical Security

- Brizo application servers are hosted on Amazon Web Services. As such, Brizo inherits the control environment which demonstrates numerous US, worldwide, and government certifications and more. Web servers and databases run on servers in secure data centers. Physical access is restricted to authorized personnel. Premises are monitored and access is logged.

Network Security

- All employees with administrative access must pass a criminal background check at every year.

Authentication

- 2FA and/or SSH keys for employees with administrative access to the servers.

Development Process

- Brizo developers have been trained in secure coding practices. Brizo application architecture includes mitigation measures for common security flaws such as the OWASP Top 10 and entries the CVE database. The Brizo application uses industry standard, high-strength algorithms including AES for all data encryption. Brizo undergoes penetration testing at least once per year.

Employee Screening and Policies

- As a condition of employment all Brizo employees with access to code, hosted services, or customer data undergo criminal background checks. All Brizo employees take mandatory security training and agree to company policies including security and acceptable use policies.

Security Issues

- At Brizo, we consider the security of our systems a top priority. We have implemented a responsible disclosure policy to ensure that problems are addressed quickly and safely.

ANNEX C: LIST OF APPROVED SUBPROCESSORS

NAME	ADDRESS OF PROCESSOR	PROCESSING ACTIVITIES	TERRITORY(IES)
Frontegg	https://frontegg.com/	BFM user authentication	https://frontegg.com/wp-content/uploads/2021/06/Frontegg-List-of-approved-subprocessors.pdf
AWS	https://aws.amazon.com/	Data storage (incl. contacts)	North Virginia, central Canada
Snowflake	https://www.snowflake.com/	Data storage (incl. contacts)	https://www.snowflake.com/legal/snowflake-sub-processors/ (les régions qu'on utilise chez AWS)
Datadog	https://www.datadoghq.com/	Server logs	https://www.datadoghq.com/privacy/ (us-east-1 (North Virginia))
Hotjar	https://www.hotjar.com/	Application usage logging	https://help.hotjar.com/hc/en-us/articles/115011639887-Data-Safety-Privacy-Security#data-storage AWS eu-west-1
Pipedrive	https://www.pipedrive.com/	CRM	Not clear (Client country and US? See below) **https://www.pipedrive.com/en/privacy#data-security**

ANNEX D: COMPETENT SUPERVISORY AUTHORITY

For the purposes of any Personal Data subject to the GDPR and/or the GDPR as implemented in the domestic law of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018, where such personal data processed in accordance with the Model Clauses, the competent supervisory authority shall be as follows:

(a) where Customer is established in an EU member state, the supervisory authority with responsibility for ensuring Customer's compliance with the GDPR shall act as competent supervisory authority;

(b) where Customer is not established in an EU member state, but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU member state in which Customer's representative is established shall act as competent supervisory authority; or

(c) where Customer is not established in an EU member state but falls within the extra-territorial scope of the GDPR without however having to appoint a representative, the supervisory authority of the EU member state in which the Data Subjects are predominantly located shall act as competent supervisory authority.

In relation to Personal Data that is subject to the U.K. GDPR, the competent supervisory authority is the United Kingdom Information Commissioner's Office, subject to the additional terms set forth in the International Data Transfer Addendum to the EU Model Clauses attached hereto as "Appendix E".

In relation to Personal Data that is subject to the data privacy laws of Switzerland, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

ANNEX E: U.K INTERNATIONAL DATA TRANSFER ADDENDUM

This U.K. INTERNATIONAL DATA TRANSFER ADDENDUM ("IDTA") forms a part of the Data Processing Addendum ("DPA") entered into by and between Brizo, Inc. ("Brizo") and the party identified as the Customer in the DPA ("Customer"). Unless otherwise specified, all capitalized terms used in this IDTA have the meanings provided in the DPA.

1. **Scope of IDTA.** The obligations set forth in this IDTA apply solely to Personal Data subject to the U.K. GDPR that is processed under the DPA ("U.K. Personal Data").
2. **Incorporation of the U.K. Addendum.** The parties agree that the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as issued by the U.K. Information Commissioner's Office under s.119A
   (1) of the U.K. Data Protection Act 2018 ("U.K. Addendum") is incorporated by reference into and forms a part of this IDTA as if fully set forth herein. Each party agrees that execution of the DPA (to which this IDTA is attached as an appendix and incorporated by reference) shall have the same effect as if the parties had simultaneously executed a copy of the U.K. Addendum.
3. **Interpretation of the Model Clauses.** For purposes of Processing U.K. Personal Data, any references in the DPA to the Model Clauses shall be read to incorporate the mandatory amendments to the Model Clauses set forth in the U.K. Addendum.
4. **Addendum Terms.** Tables 1 through 4 of the U.K. Addendum shall be completed as follows:
   (a) In Table 1 of the U.K. Addendum, the "Start Date" shall be the Effective Date of the DPA, and the details and contact information for the "data exporter" and the "data importer" shall be as specified in Appendix I of the DPA.
   (b) In Table 2 of the U.K. Addendum:
      i. The version of the Model Clauses incorporated by reference into the DPA shall be the version applicable to this IDTA.
      ii. Those provisions of the Model Clauses applicable under Module Two shall apply to this IDTA.
      iii. The optional clauses and provisions of the Model Clauses applicable to this IDTA shall be those clauses and provisions specified in Section 2.3 of the DPA.

(c) In Table 3 of the U.K. Addendum, the information required in Annexes I (both 1A and 1B), II, and III shall be as provided in Appendices A, B, and C of the DPA, respectively.

(d) In Table 4 of the U.K. Addendum, if the ICO issues any revisions to the U.K. Addendum after the Effective Date ("ICO Revision"), Customer and Brizo shall each have the right to terminate this IDTA in accordance with the U.K. Addendum, the DPA, and the Agreement. Upon such termination of this IDTA:

i. Brizo shall cease its Processing of the U.K. Personal Data; and

ii. Each party shall follow the processes described in Section 2.11 of the DPA with respect to the U.K. Personal Data.

Notwithstanding the foregoing, termination of this IDTA in the event of an ICO Revision shall not terminate the DPA, the Agreement, and/or the obligations of either party arising thereunder with respect to Personal Data other than U.K. Personal Data, except and unless expressly agreed by and between the parties.

5. **No Amendments.** The terms of the U.K. Addendum have not been amended in any way except as expressly stated herein.

SIGNATURE AREA

CUSTOMER	BRIZO, INCORPORATED
Signature:	**Signature:**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**