PRIVACY SCHEDULE (Supplier)

This Data Privacy Schedule ("**Addendum**") is made and entered into by and between LevelBlue, LLC or the applicable LevelBlue affiliate identified in the Agreement (collectively, "**LevelBlue**") a Delaware limited liability company, and the supplier specified below. ("**Supplier**").

LevelBlue:	**LevelBlue, LLC.**
Authorized Representative Signature:	By:
Printed Name:	
Notice (Email):	Legal@LevelBlue.com
Title:	
Date:	

Supplier:	
Authorized Representative Signature:	By:
Printed Name:	
Notice (Email):	
Title:	
Date:	

This Addendum supplements the Master Agreement or other agreement executed with Supplier (the "**Agreement**") by and between LevelBlue and Supplier (each a "**Party**" and collectively the "**Parties**"). This Addendum is incorporated into and applies to Supplier's service offerings purchased by LevelBlue. Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

Definitions

1.1 "**Applicable Law(s)"** means any state, federal or foreign law(s), rule(s) directive(s), statute(s) regulation(s) or binding obligation(s) of a Global Jurisdiction that govern the handling, security, availability, integrity, confidentiality and Processing of Personal Data, such as, without limitation to the Regulation (EU) 2016/679 General Data Protection Regulation ("**GDPR**"), and the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA/CPRA**").

1.2 "**Authorized Employee"** means an employee of Supplier or a Supplier Affiliate who has a need to know or otherwise access Personal Data in order to enable Supplier to perform its obligations under this Addendum or the Agreement and who has undergone appropriate background screening and training by Supplier.

1.3 "**Authorized Person**" means an Authorized Employee of a Party or Authorized Subcontractor of the Party.

1.4 "**Authorized Subcontractor**" means a third-party subcontractor, agent, reseller, or auditor engaged by Supplier, or employee of same, that has a need to know or otherwise access Personal Data to enable Supplier to perform its obligations under this Addendum or the Agreement and that has been previously approved by LevelBlue in writing to do so, and who is bound in writing by a data processing agreement pursuant to which their duties and obligations to protect Personal Data are in strict accordance with the terms hereof.

1.5 "**Controller**" is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

1.6 "**Data Subject**" is an identified or identifiable natural person, 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.

1.7 "**Data Subject Rights**" shall mean the rights afforded to Data Subjects under Applicable Laws. Rights include without limitation: Right of Access; Right of Rectification; Right of Erasure; Right to Restrict Processing; Right to Data Portability; Right to Object; Right to Withdraw.

1.8 "**Downstream Entity**" means Supplier and any approved Authorized Subcontractor Processing Personal Data on Supplier's behalf.

1.9 "**Extended EEA Country**" means either a country within the European Economic Area ("**EEA**"); Switzerland; or the United Kingdom, and "Extended EEA Countries" means the foregoing countries collectively.

1.10 "**Global Jurisdiction**" means collectively Extended EEA Countries and any other country where the Parties operate, collect, store, transfer or Process Personal Data, subject to Applicable Laws, industry regulations, or contractual obligations.

1.11 "**Industry Standards**" means the then-current industry best data protection and data processing practices relating to the Processing of the Personal Data, including where appropriate, ISO 27001, SOC 2, or equivalent standards.

1.12 "**Instruction**" means a direction issued by LevelBlue to Supplier and/or any Authorized Person, documented either in textual form (including without limitation by e-mail) or by using a software or online tool, regarding the Processing of Personal Data.

1.13 "**Personal Data**" means any information relating to a Data Subject.

1.14 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.15 "**Personal Information**" shall have meaning under CCPA/CPRA and where used herein shall be included within Personal Data where applicable.

1.16 "**Process**" or "**Processing**" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, transfer or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.17 "**Processor**" is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

1.18 "**Restricted Transfer**" means a transfer of Personal Data from any country or recipient: (i) not deemed by the European Commission or other Global Jurisdiction as providing an adequate level of protection for Personal Data, and (ii) not covered by or a suitable framework or certification recognized by the relevant Supervisory Authority or Applicable Law as providing an adequate level of protection for Personal Data.

1.19 "**Security Incident**" or "**Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

1.20 "**Services**" shall have the meaning set forth in the Agreement.

1.21 "**Standard Contractual Clauses**" means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. Published under document number C/2021/3972.

1.22 "**Supervisory Authority**" means an independent public authority which is established pursuant to Article 51 of the GDPR.

1.23 "**Technical and Organizational Security Measures**" means measures taken by Supplier and Authorized Persons aimed at (i) ensuring the confidentiality, security, integrity, and availability of Personal Data, including protecting against an Incident, a Personal Data Breach, or other accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access to Personal Data (in particular where Processing involves the transmission of Personal Data over a network) and other unlawful forms of Processing and/or (ii) assisting and enabling LevelBlue to comply with its obligations to respond to requests by Data Subjects to exercise their Data Subject Rights.

2 Indemnity

2.1 Supplier shall, at its own expense, protect, defend, indemnify and hold harmless LevelBlue and its officers, directors, employees, successors, assigns, distributors, contractors, agents, affiliates and customers, from all claims or actions, damages, liabilities, assessments, losses, costs, and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses and breach notification expenses) arising out of or resulting from (a) any breach by Supplier of its warranties or representations in this Addendum, (b) any acts and omissions of any Authorized Subcontractors with respect to the Processing of any Personal Data; or (c) any Incident or Personal Data Breach (collectively, "**Claims**").

2.2 LevelBlue shall provide Supplier with prompt written notice of any Claim. Upon receipt of any such notice, Supplier must immediately take all necessary and appropriate action to protect LevelBlue's interests with regard to any Claims. LevelBlue shall provide reasonable cooperation, information, and assistance in connection with any Claim (except that failure to do so shall only excuse Supplier from its obligations to the extent such failure materially prejudiced the defense of the Claim). Supplier shall have sole control and authority to defend, settle or compromise any Claim, provided that Supplier shall not make any settlement that requires a materially adverse act or admission by LevelBlue without LevelBlue's written consent (such consent not to be unreasonably delayed, conditioned or withheld). If Supplier provides counsel for the defense of any Claim and LevelBlue, in its sole discretion, determines that such counsel is unacceptable or that a conflict of interest exists between LevelBlue and such counsel, LevelBlue may request Supplier replace the counsel. If Supplier fails to timely replace counsel, the Supplier agrees that its counsel shall work in good faith with LevelBlue's counsel until the Claim is resolved.

3 Processing of Data

3.1 Supplier acts solely as Processor unless otherwise expressly agreed.

3.2 Supplier agrees to comply with this Addendum, at no additional cost to LevelBlue, at all times during the term of the Agreement. Any failure by Supplier to comply with the obligations set forth in this Addendum, a Security Incident or any Personal Data Breach, will be considered a material breach of the Agreement, and LevelBlue will have the right, without limiting any of the rights or remedies under this Addendum or the Agreement, or at law or in equity, to immediately terminate the Agreement for cause.

3.3 Supplier acknowledges that LevelBlue may be the Controller of the Personal Data or may be a Processor of the Personal Data on behalf of another Controller.

3.4 The rights and obligations of LevelBlue with respect to Processing are described herein and in the Agreement. The duration of the Processing shall be for the term of the Agreement, unless earlier terminated. The categories of Data Subject shall include LevelBlue end users/customer and LevelBlue employees and contractors.

3.5 The types of Personal Data collected may include without limitation: Individual Name; Employing Company; Phone; Email address; Mailing address, including country; User identifiers; Session logs; Firewall events; Log in attempts; Incident reports; Security alerts; IP address; Log data; and Device identifiers.

3.6 Supplier acknowledges and agrees that it shall only Process Personal Data for the limited and specified purpose of Processing Personal Data on behalf of LevelBlue solely pursuant to the Agreement and in strict compliance with the terms and conditions set forth in this Addendum and in any Instructions.

3.7 Supplier represents and warrants that its Processing of Personal Data does and will comply with all Applicable Laws.

4 Security of Data

4.1 At a minimum, and without limiting the foregoing, Supplier represents and warrants that it shall maintain all Personal Data in strict confidence, using a degree of care and Technical and Organizational Security Measures that meet or exceed applicable Industry Standards and ensure a level of security appropriate to the particular risks of accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access of Personal Data presented by the Processing and the Personal Data (collectively, "**Risks**"), including (i) limiting access to Personal Data to Authorized Persons only; (ii) ensuring that all Authorized Persons are made aware of the confidential nature of Personal Data before they may access such data; (iii) securing its physical, technical, and administrative infrastructure, including all relevant business facilities, data centers, paper files, servers, networks, platforms, databases, cloud computing resources, back-up systems, passwords and credentials, hardware, and mobile devices; (iv) implementing authentication and access controls within all relevant media, applications, networks, operating systems and equipment; (v) encrypting Personal Data at all times and Personal Data when transmitted over public or wireless networks or where otherwise appropriate in light of the Risks; (vi) strictly segregating Personal Data from information of Supplier or its employees or other customers; (vii) maintaining appropriate personnel security and integrity procedures and practices, as set forth in Section 5 – Authorized Persons; (viii) maintaining and regularly testing processes for restoring the availability and access to Personal Data in a timely manner in the event of an Incident or Suspected Incident; (ix) regularly testing, assessing, and evaluating the effectiveness of all Technical and Organizational Security Measures; and (x) any other measures necessary to ensure the ongoing confidentiality, integrity, and availability of Personal Data and the ongoing security and resilience of systems and services used for Processing.

4.2 Upon LevelBlue's written request, or, upon the termination or expiration of the Agreement for any reason, Supplier shall, and shall ensure that all Authorized Persons, (i) promptly and securely dispose of or return to LevelBlue in an encrypted format, at LevelBlue's choice, all copies of Personal Data, including backup or archival copies, and (ii) promptly certify in writing to LevelBlue when the measures described in subsection (i) hereof have been completed. Supplier shall, and shall ensure that all Authorized Persons, comply with all Instructions provided by LevelBlue with respect to the return or disposal of Personal Data. Any disposal of Personal Data must ensure that such data is rendered permanently unreadable and unrecoverable. Supplier and/or Authorized Persons shall be excused from performing the foregoing obligations only if, and solely to the extent that, Applicable Law(s) explicitly prevent them from doing so.

5 Authorized Persons

5.1 Supplier represents, warrants, and covenants that it has previously informed LevelBlue and obtained its prior written consent to any Processing of Personal Data by third parties other than Supplier and its Authorized Employees. Supplier shall promptly send LevelBlue a copy of any Authorized Subcontractor agreement relevant to this Addendum.

5.2 Supplier shall perform appropriate screening of all Authorized Persons, including without limitation background checks in accordance with Applicable Laws, and shall ensure the reliability and appropriate training of all Authorized Persons.

5.3 Supplier represents, warrants, and covenants that it has executed written agreements with each Authorized Subcontractor that bind them to all obligations set forth in this Addendum with respect to the Processing of the Personal Data.

5.4 Supplier represents, warrants, and covenants that it has executed confidentiality agreements with each Authorized Person that prevents them from disclosing or otherwise Processing, both during and after their engagement by Supplier, any Personal Data except in accordance with their obligations in connection with the Services.

5.5 Supplier shall be fully responsible for the acts and omissions of Authorized Subcontractors and any other of its subcontractors, independent contractors, and other service providers to the same extent that Supplier would itself be liable under this Addendum had it conducted such acts or omissions, and shall fully indemnify LevelBlue for all losses arising from or related to such acts and omissions.

6 Incident and Data Breach

6.1 Supplier shall notify LevelBlue of a Personal Data Breach without undue delay, and in no event later than twenty-four (24) hours after becoming aware of any Security Incident or Personal Data Breach. If Supplier becomes aware of any Security Incident or a Personal Data Breach, Supplier shall notify LevelBlue pursuant to Section 6.2.

6.2 Supplier shall notify LevelBlue immediately upon becoming aware of a Personal Data Breach and shall, in a written report, provide sufficient information to enable LevelBlue to comply with its obligations under Applicable Laws with respect to such Personal Data Breach, including any obligation to report or notify such Personal Data Breach to Supervisory Authorities and/or Data Subjects, as applicable. Such report will include (i) a description of the nature of the Personal Data Breach, (ii) the categories and approximate number of Data Subjects and Personal Data sets affected or alleged to be affected, (iii) the likely consequences of the Personal Data Breach, and (iv) any measures that have been or may be taken to address and mitigate the Personal Data Breach.

6.3 As soon as reasonably practicable after providing the report described in Section 6.2, Supplier shall provide LevelBlue with a comprehensive report on its initial findings regarding the Personal Data Breach, and thereafter shall provide regular updates describing subsequent findings with respect to such Personal Data Breach. As soon as reasonably practicable after Supplier has concluded its examination of the Personal Data Breach, it shall provide LevelBlue with a comprehensive final report regarding the Personal Data Breach.

6.4 Supplier and/or any relevant Authorized Subcontractor shall use its best efforts to immediately mitigate and remedy any Personal Data Breach, and prevent any further Personal Data Breach or recurrence thereof, at Supplier's own expense and in accordance with Applicable Laws.

6.5 Neither Supplier nor any Authorized Subcontractor shall publicly disclose any information regarding any Suspected Incident, Incident or Personal Data Breach without LevelBlue's prior written consent, except that Supplier and any relevant Authorized Subcontractor may disclose any Personal Data Breach to (i) its own employees, customers, advisors, agents, or contractors, or (ii) where and to the extent explicitly compelled to do so by Applicable Laws, to applicable Supervisory Authorities and/or Data Subjects without LevelBlue's prior written consent.

6.6 Supplier and/or any relevant Authorized Subcontractor shall, at Supplier's expense, fully cooperate with LevelBlue and provide any assistance necessary for LevelBlue to comply with any obligations under Applicable Laws with respect to a Personal Data Breach, including obligations to report or notify a Personal Data Breach to Supervisory Authorities and/or Data Subjects. Such assistance may include drafting disclosures, press releases and/or other communications for LevelBlue with respect to such Personal Data Breach.

6.7 Supplier shall indemnify, defend, and hold harmless LevelBlue from and against any and all claims, demands, actions, liabilities, damages, losses, fines, penalties, settlements, judgments, costs, and expenses (including reasonable attorneys' fees and costs) (collectively, "Losses") arising out of or related to:

6.8 Any unauthorized access to, disclosure of, or loss of Personal Data resulting from Supplier's acts, omissions, negligence, willful misconduct, or failure to comply with Applicable Laws or contractual obligations;

6.9 Any failure by Supplier to implement and maintain appropriate Technical and Organizational Security Measures to protect Personal Data in accordance with Applicable Laws and Industry Standards;

6.10 Any breach of confidentiality, privacy, or data protection obligations under this Agreement; and

6.11 Any regulatory investigations, fines, penalties, or third-party claims, including claims from data subjects, regulators, or customers, arising from Supplier's Incident, Personal Data Breach or non-compliance.

6.12 Supplier shall assume full responsibility for all costs associated with the investigation, notification, mitigation, credit monitoring, remediation, and legal defense arising from any Incident, Personal Data Breach or unauthorized disclosure attributable to Supplier. Supplier shall not enter into any settlement or resolution of any claim that imposes any liability, obligation, or admission of wrongdoing on the Indemnified Parties without LevelBlue's prior written consent.

6.13 In the event of a Personal Data Breach or data processing infringement, Supplier will provide LevelBlue with reasonable cooperation, communication and assistance necessary for LevelBlue to comply with its obligations under Applicable Laws with respect to notifying (i) the relevant Supervisory Authority, and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

6.14 This indemnification obligation shall survive the termination or expiration of this Agreement.

7 Rights of Data Subjects

7.1 Supplier shall, to the extent permitted by Applicable Laws, provide all necessary assistance to LevelBlue in responding to requests by Data Subjects to exercise Data Subject Rights, including, as applicable and without limitation to, a Data Subject's right to: (a) confirm whether his or her Personal Data has been or is being Processed; (b) access a copy of all Personal Data of his or hers that has been or is being Processed; (c) rectify or supplement his or her Personal Data; (d) transfer his or her Personal Data to another controller or designated recipient, where applicable; (e) confirm that his or her Personal Data has been or is being subject to Processing that constitutes automated decision-making; (f) restrict or cease the Processing of his or her Personal Data; and (g) withdraw consent to the Processing of his or her Personal Data held by Supplier. Such assistance shall also include (h) maintaining records sufficient to demonstrate Supplier's performance of its obligations under Applicable Laws with respect to Data Subject Rights, (i) promptly notifying LevelBlue if Supplier or an Authorized Subcontractor receives a request from a Data Subject to exercise a Data Subject Right and refraining from responding to such requests (and ensuring that Authorized Subcontractors refrain from responding to such requests) except upon receipt of, and in accordance with, Instructions from LevelBlue, and (j) informing LevelBlue in the event that Applicable Laws or any judicial, law enforcement, or Supervisory Authority operate to prevent Supplier (or any Authorized Subcontractor) from performing the obligations described in this Section 7.1, before Supplier (or an Authorized Subcontractor) responds to a request to exercise a Data Subject Right.

8 Transfers of Personal Data

8.1 Where required, the SCCs shall be completed in accordance with applicable law, including governing law and forum requirements. Where UK or Swiss transfer restrictions apply, the Parties shall implement the UK International Data Transfer Addendum, Swiss Addendum, or other lawful transfer mechanisms as required.

8.2 The Parties hereby acknowledge and agree that the Standard Contractual Clauses set forth in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (GDPR), including the applicable module(s) relevant to their data transfer arrangement, and to implement any necessary supplementary measures to ensure an equivalent level of data protection as required under GDPR ("**SCCs**") shall apply to any Restricted Transfers made in connection with the Services.

8.3 Supplier represents, warrants, and covenants that no Authorized Subcontractor will be permitted to undertake or receive a Restricted Transfer before executing the Standard Contractual Clauses.

8.4 Supplier represents and warrants that every Restricted Transfer made by Supplier or any Authorized Subcontractor shall be undertaken in accordance with the Standard Contractual Clauses.

9 Actions and Access Requests

9.1 Upon LevelBlue's request, Supplier shall make available to LevelBlue all information available to Supplier and to Authorized Subcontractors that LevelBlue reasonably deems necessary to demonstrate compliance by LevelBlue with its obligations under Applicable Laws (including in particular the GDPR and CCPA/CPRA, when effective) relating to the Personal Data and the Processing conducted by Supplier and Authorized Subcontractors.

9.2 Supplier acknowledges and warrants that the processing of Personal Data under this Addendum does not and will not infringe upon any third-party intellectual property rights.

9.3 Upon LevelBlue's request, Supplier shall provide all necessary assistance to LevelBlue in connection with any request to comply with any Applicable Law that LevelBlue determines (in its sole discretion) it must conduct or cause to be conducted in order to comply with Applicable Laws.

10 Audit Rights

10.1 Supplier shall use external auditors to verify the adequacy of its security measures. This audit (a) will be performed at least annually; (b) will be performed by independent third-party security professionals at Supplier's selection and expense; and (c) will result in the generation of an audit report ("**Report**"), which will be Supplier's Confidential Information. Supplier shall maintain complete and accurate records in connection with Supplier's performance under this Addendum, and shall retain such records for a period of three (3) years after the termination or expiration of the Agreement.

10.2 At LevelBlue's written request, Supplier will provide LevelBlue with a confidential Report so that LevelBlue can reasonably verify Supplier's compliance with the security obligations under this Addendum.

11 Flow-Down Data Protection Obligations for Downstream Entities

11.1 Only Process Personal Information as instructed by LevelBlue and solely for the purposes specified in this Addendum or the Agreement and its associated statements of work or equivalent.

11.2 The Downstream Entity is not permitted to sell, share, or use Personal Information for commercial or other unauthorized purposes.

11.3 The Downstream Entity is not permitted to combine Personal Information received on behalf of LevelBlue with other data unless authorized by law.

11.4 The Downstream Entity shall not Process Personal Information outside of the scope of the LevelBlue and Downstream Entity business relationship.

11.5 The Downstream Entity shall not cause LevelBlue to be in breach of its contractual obligations under other agreements or Data Protection Laws.

11.6 Technical and Organizational Measures

The Downstream Entity shall implement technical and organizational measures at least as protective as industry standards which include without limitation:

- 11.6.1 Data encryption
- 11.6.2 Pseudonymization
- 11.6.3 Network segmentation
- 11.6.4 Role-based access control
- 11.6.5 Logging and monitoring
- 11.6.6 Remote work controls
- 11.6.7 Secure deletion protocols
- 11.6.8 Multi-factor authentication

11.7 Support LevelBlue in responding to requests from contractual and other regulatory obligations relating to:

- 11.7.1 Access/Right to Know
- 11.7.2 Deletion

11.7.3 Correction
11.7.4 Limitation of Use

11.8 Comply with request timelines without undue delay and sufficient to enable LevelBlue to comply with Applicable Law.
11.9 Maintain auditable records of all actions taken to comply with such requests.
11.10 Maintain complete and accurate records demonstrating compliance with this Addendum.
11.11 Permit audits by LevelBlue (or their designated representatives) to verify compliance.
11.12 Cooperate with Data Access or Data Remediation Audits, including providing access to relevant systems, records, personnel, and subcontractors.
11.13 International Data Transfers:

11.13.1 If the Downstream Entity processes data originating from:
11.13.2 EEA: The Downstream Entity must comply with Standard Contractual Clauses (SCCs) Module Two or Three as applicable.
11.13.3 UK: The Downstream Entity must comply with the UK IDTA Addendum.
11.13.4 Brazil: Applicable LGPD compliant transfer mechanisms.
11.13.5 Other countries: The Downstream Entity must comply with applicable local data protection laws and any mechanisms required for data export.

11.14 Notify LevelBlue of any subcontract relationship or transfers on behalf of LevelBlue as applicable to provide the services under this Addendum, Agreement, its associated statements of work or equivalent .
11.15 Complete Transfer Impact Assessments (TIAs) when applicable.
11.16 Designate a Data Protection Officer or equivalent responsible contact. This contact must be available for communications between the parties and coordination of audits, investigations, and data subject requests.
11.17 Supplier shall only process data until the Personal Data is no longer needed for the purposes for which it was collected, which shall be at the end of the term of this Agreement at the latest unless otherwise needed for Data Protection Law obligations.
11.18 Categories of Personal Data subjects may consist of employees, representatives of LevelBlue, business contact data, electronic communications metadata, device identification data, geolocation data and application content for the ongoing processing operations of performance of services, management of network devices, network utilization, management of information, electronic communications in order to perform services under this Addendum, Agreement or any applicable statement of work or equivalent.

12 Miscellaneous

12.1 This Addendum may be amended or modified only by a writing signed by both Parties. Supplier acknowledges and agrees that LevelBlue (whether it is acting as a controller or a processor on behalf of another controller) may disclose this Addendum to third parties (including other controllers, data subjects and regulators) for purposes of demonstrating compliance with Applicable Laws.
12.2 The Parties hereby acknowledge and agree that any remedies arising from any Personal Data Breach or any breach by Supplier or any Authorized Person under the terms of this Addendum are not and shall not be subject to any limitation of liability provision that applies to Supplier under the Agreement.
12.3 This Addendum shall be governed by the law of the same jurisdiction as the Agreement, except where and to the extent that Applicable Laws require that the Addendum be governed by the law of another jurisdiction.

This Addendum shall remain in effect for the duration of Supplier's provision of services under the Agreement. Notwithstanding the termination or expiration of the Agreement, if Supplier retains any Personal Data beyond the Service or Agreement term, this Addendum shall survive and remain in full force and effect until such Personal Data is returned or securely destroyed in accordance with the terms of this Addendum. Supplier shall not retain, use, or disclose Personal Data beyond the permitted retention period except as required by Applicable Law, in which case Supplier shall continue to comply with the obligations set forth in this Addendum.