DATA PROCESSING AGREEMENT

Effective Date: April 30, 2025

1 **Introduction.** This Data Processing Agreement (this "**DPA**") forms an integral part of the underlying service agreement between the parties as the provider ("**Provider**") and recipient ("**Customer**"), respectively, of services described in the agreement when such agreement explicitly incorporates by reference this DPA (such agreement, including any terms of service, order form, addendum, Service Details, or other documentation incorporated therein, collectively, the "**Agreement**"). Provider and Customer are each a "**Party**" and collectively the "**Parties**" to this DPA.

2 **Roles of the Parties.** Subject to applicable Data Protection Laws, the Parties hereby acknowledge and agree that:

2.1 With respect to Provider's Processing of Customer Personal Data, Customer shall be the Controller, and Provider shall be the Processor.

2.2 If Customer is a Processor on behalf of a third party, Provider is a Sub-processor, and Customer represents and warrants that Customer's instructions to Provider on Processing Customer Personal Data, including Customer's appointment of Provider as a Sub-Processor, have been fully authorized by the respective Controller.

2.3 Each Party is an independent Controller with regard to business operations incidental to providing the Service, which may include account management, accounting, tax, billing, audit, compliance, and investigation or prevention of fraud, spam, or wrongful or unlawful use or as further provided under applicable law. Provider may also act as Controller for other Processing beyond the abovementioned scope, if and to the extent authorized by Customer under the Agreement.

3 **General Compliance Obligations.**

3.1 When Provider Processes Customer Personal Data on behalf of Customer, this DPA, along with the Agreement, constitute documented instructions from Customer on which Provider may Process Customer Personal Data. Provider shall:

3.1.1 if and to the extent required by Data Protection Laws, inform Customer if, in Provider's reasonable opinion, any Processing instructions from Customer infringe such Data Protection Laws;

3.1.2 comply, and with reasonable efforts assist Customer in complying, with Data Protection Laws;

3.1.3 not perform its obligations under the Agreement in such a way as to knowingly cause Customer to breach any of its obligations under applicable Data Protection Laws;

3.1.4 obligate its employees, Sub-processors, and any other third party authorized by Provider to Process Customer Personal Data in connection with the Service to written confidentiality obligations or ensure the same are under appropriate statutory obligations of confidentiality;

3.1.5 contractually obligate its Sub-processors and any other third parties authorized to Process Customer Personal Data on Provider's behalf to provide substantially the same level of protection for Customer Personal Data as provided in this DPA and as required by Data Protection Laws;

3.1.6 where required under Data Protection Laws, take reasonable steps, in light of the deadlines provided for in Data Protection Laws, to promptly notify and provide reasonable cooperation to Customer if Provider receives any requests in connection with its Processing of Customer Personal Data from: (i) Data Subjects to exercise their rights granted by Data Protection Laws; or (ii) any governmental, regulatory or supervisory authority or legal judicial process, provided such notice is not prohibited by law or court order;

3.1.7 upon Customer's reasonable request, where such means and assistance are not already in Customer's control or possession, and to the extent required by Data Protection Laws, provide assistance and information necessary for Customer to comply and demonstrate Customer's compliance with its legal obligations with respect to:

(A) requests for audits or assessments, at Customer's cost and expense, to occur no more than annually, or more frequently if due to a legal requirement, a Data Breach, or a demand from applicable regulatory authority, provided that: (i) any audits or assessments shall be conducted during Provider's normal business hours upon advance written notice at times to be agreed by Provider, (ii) Provider's written approval for the use of any third-party auditors shall be obtained in advance, in writing, and not to be unreasonably withheld, and (iii) Customer shall ensure that information provided by Provider, or otherwise revealed in the course of any such audit or assessment, will be treated as Provider's Confidential Information. Neither Provider nor any third-party auditor shall have the right to access Provider's or its other customers' or third parties' Personal Data or Confidential Information;

(B) information needed for Customer's records of Processing activities and data protection impact assessments (such scope as determined by Data Protection Laws); and

(C) security information relating to the Processing of Customer Personal Data.

3.2 In connection with the Service, Customer shall comply with Data Protection Laws, any additional terms described in the applicable Service Details such as third-party licensor or flow down terms, and this DPA, and ensure all instructions and Personal Data given by Customer to Provider will be in compliance with Data Protection Laws.

4 **Data Security.**

4.1 The Parties agree that Provider will implement and maintain the Technical and Organizational measures as described in Exhibit 1 (TECHNICAL AND ORGANIZATIONAL MEASURES) to this DPA.

4.2 Data Breach:

4.2.1 If either Party discovers or learns of a Data Breach, it shall take commercially reasonable, appropriate, and prompt steps to: (a) investigate and mitigate the Data Breach; (b) notify the other Party of such Data Breach; (c) furnish necessary and relevant details of the Data Breach as may be available; (d) provide reasonable assistance, as needed, in the investigation and mitigation of the Data Breach; and (e) provide information and assistance, as needed, in meeting a Party's legal obligations, including any applicable obligations to notify individuals, regulators and/or other parties.

4.2.2 Unless prohibited by applicable law or court order, each Party shall notify the other Party of any third-party legal process relating to any Data Breach, including but not limited to any legal process initiated by any governmental entity or other party.

4.2.3 A Party's cooperation or obligation to report or respond to Data Breaches under this DPA shall not be deemed an acknowledgment by a Party of any fault or liability with respect to a Data Breach.

5 **Sub-processors.**

5.1 Customer hereby gives general consent to Provider to engage the Sub-processors, including Provider's affiliates, set forth in the Service Details. Before amending the list of Provider Sub-processors identified in the Service Details, Provider will notify Customer as described in the Service Details, and Customer authorizes Provider to use any such Sub-processor to Process Customer Personal Data unless Customer objects within thirty (30) calendar days of such notification. Any such objection must be based on reasonable grounds. If such objection is justified, Customer and Provider will work together to find a mutually acceptable resolution to such objection.

5.2 Where a Sub-processor fails to fulfil its data protection obligations under such written agreement or Data Protection Laws, Provider will remain responsible to Customer for the performance of such obligations.

6 **International Data Transfers.**

6.1 With regard to countries, regions, or territories with Data Protection Laws requiring a condition for the valid export of Personal Data, or any subset or category of data within the Customer Personal Data (such countries, regions, or territories, “**Limited Transfer Region(s)**” and such data, to the extent restricted, “**Limited Transfer Data**”), Provider may not receive and Process such Limited Transfer Data outside of a Limited Transfer Region unless Provider (or its relevant Sub-Processor(s)) adopts measures, safeguards, or mechanisms recognized by such Data Protection Laws as satisfying such condition (each, a “**Valid Mechanism**”). Limited Transfer Data transferred to third countries, regions or territories that are not deemed by the applicable authorities as providing an adequate level of data protection shall be subject to Exhibit 2 of this DPA (including, as applicable, any other Exhibits referred to in Exhibit 2).

6.2 Customer agrees that the transfer mechanisms in Exhibit 2 or any other Exhibit are each a Valid Mechanism and that Provider may transfer Limited Transfer Data outside of a Limited Transfer Region pursuant to such Exhibits.

6.3 The Parties agree that to the extent any additional Valid Mechanism is required to export data to a third country, region or territory, or if the Valid Mechanism agreed upon under this DPA is substituted, replaced, or no longer recognized under Data Protection Laws as satisfying the conditions for valid export, Provider will use another Valid Mechanism.

6.4 Notwithstanding the availability of a Valid Mechanism, where implementation of such Valid Mechanism is not commercially reasonable, Provider may discontinue the Service in the applicable region(s) without penalty, subject to any provisions in the Agreement applicable to discontinuation of the Service, if any.

7 **Retention and Deletion of Customer Personal Data.** Upon termination or expiration of the Agreement or Customer’s written request to delete Customer Personal Data, Provider shall cease to Process any Customer Personal Data beyond passively storing such data, and delete all Customer Personal Data under Provider’s possession or control or, if technically feasible, provide Customer the ability to delete such Customer Personal Data directly through tools or functionality made available by Provider; except (a) where such deletion is not permitted under applicable laws (including Data Protection Laws) or the order of a governmental or regulatory body, (b) where Provider retains such data for compliance with any legal obligation, (c) where Provider’s then-current data retention or similar back-up system stores Customer Personal Data, provided such data will remain protected in accordance with the measures described in the Agreement and this DPA, or (d) where Provider is a Controller.

8 **Miscellaneous.**

8.1 **Termination and Survival.** Upon termination or expiration of the Agreement, this DPA shall automatically and immediately expire as it applies to such Agreement, provided, however, the provisions of this DPA that, by their terms, require performance after the termination or expiration of this DPA, or apply to events that may occur after the termination or expiration of this DPA, will survive.

8.2 **Governing Law; Conflicts of Law; Severance.** Without prejudice to clauses 17 (governing law) and 18 (choice of forum and jurisdiction) of the Incorporated SCCs (if applicable), the Parties hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated in the Agreement (without reference to its conflict of laws requirements), unless otherwise required by Data Protection Laws. To the extent any court or governmental entity with competent jurisdiction determines that a provision of this DPA is invalid or unenforceable, the Parties agree and intend that such provision should be (a) amended solely as necessary to bring it back into force in a manner consistent with the Parties’ manifest intent, or if that is not possible (b) severed from the DPA in a manner to give maximum legal force and effect to the remaining provisions.

8.3 **Updates to the DPA.** Provider reserves the right to update this DPA where such change is strictly required by any applicable Data Protection Law, court order or regulatory guidance. Provider shall inform Customer of such changes (email shall suffice) and give Customer an opportunity to object within a reasonable period of time from the delivery of such notice of change. Customer and Provider will, in good faith, resolve any objections raised by Customer. Unless Customer has objected as set forth in this paragraph, the changes to this DPA shall become effective thirty (30) days from the date Provider notifies Customer of such changes (or such earlier period as required by Data Protection Laws, court order, or guidance issued by a governmental regulator).

8.4 **Conflict.** If there is any conflict or inconsistency between any terms comprising the Agreement, the following order of priority shall apply: the standard contractual clauses referenced in Exhibit 2 to this DPA (the "Incorporated SCCs"); the jurisdiction-specific terms, e.g., in Exhibits 2, 3 and 4 to this DPA; the main body of this DPA; the remainder of the Agreement. Any ambiguity in this DPA shall be resolved to permit the Parties to comply with mandatory obligations under Data Protection Laws.

8.5 **Applicability.** If Customer is subject to the federal U.S. Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as a Covered Entity or Business Associate (as such terms are defined by HIPAA), Customer shall not provide any Personal Data that constitutes Protected Health Information ("PHI") (as such term is defined by HIPAA) to Provider pursuant to the Agreement or this DPA. In the event that Customer desires to provide PHI (or access thereto) to Provider pursuant to the Agreement, Customer shall notify Provider in writing of its intent to provide such PHI (or access thereto). Provider may, in its sole discretion, agree to receive such PHI (or access thereto); provided, however, that the Parties shall enter into a separate Business Associate Agreement ("BAA") prior to Customer's provision of PHI (or access thereto) to Provider. Customer acknowledges and agrees that this DPA does not apply to Personal Data to the extent such Personal Data is regulated as PHI under HIPAA and that, in such case, the BAA shall govern.

9 **Definitions.** The capitalized terms of this DPA shall have the meanings set forth below, unless otherwise specified in this DPA. Capitalized terms used but not defined in this DPA shall have the meaning given to them in the Agreement. Cognates of all terms shall be construed accordingly.

9.1 "**California Consumer Privacy Act**" means the California Consumer Privacy Act of 2018 (as amended) and final regulations issued thereunder ("**CCPA**").

9.2 "**Chinese Data Protection Law**" means the PRC Personal Information Protection Law, the PRC Cybersecurity Law, the PRC Data Security Law, their supporting regulations and standards, and other laws governing privacy and data protection matters in the People's Republic of China (for the purposes of this Addendum, excluding Hong Kong, Macau and Taiwan; "**China**").

9.3 "**Confidential Information**" has the meaning given to it (or a substantially similar term), in the Agreement.

9.4 "**Controller**" means 'controller' as defined in the GDPR and other substantially similar roles in other Data Protection Laws.

9.5 "**Customer Personal Data**" means any Personal Data made available by or on behalf of Customer to Provider for Provider's Processing on behalf of Customer, or collected by Provider solely on behalf of Customer, in connection with the Service.

9.6 "**Data Breach**" means any unauthorized interference with the availability of, or any unauthorized, unlawful or accidental loss, misuse, destruction, alteration, acquisition of, access to, disclosure of, or damage to, Customer Personal Data.

9.7 "**Data Protection Laws**" means all applicable transnational, national, federal, state or local laws (statutory, common or otherwise), treaties, conventions, ordinances, codes, rules and regulations of any applicable jurisdiction related to privacy, personal data protection and information security, to the extent such laws, treaties, conventions, ordinances, codes, rules and regulations govern and are binding upon the relevant Party in its performance of its obligations or exercise of its rights under the Agreement, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the GDPR as incorporated into UK law, the CCPA and the Chinese Data Protection Law.

9.8 “**Data Subject**” means an identified or identifiable natural person about whom Personal Data is Processed in connection with the Service, or as otherwise defined (including under similar terms such as ‘consumer’) under Data Protection Laws.

9.9 “**Personal Data**” means ‘personal data’ as defined in the GDPR or other substantially similar terms in other Data Protection Laws such as ‘personal information’.

9.10 “**Processing**” means the performance of any operation or set of operations upon data, whether or not by automatic means, such as collection, receipt, recording, organization, structuring, alteration, use, transmission, access, sharing, provision, disclosure, distribution, copying, transfer, storage, management, retention, deletion, combination, restriction, summarizing, aggregation, correlation, inferring, derivation, analysis, adaptation, retrieval, consultation, destruction, or disposal.

9.11 “**Processor**” means ‘processor’ as defined in the GDPR and other substantially similar roles in other Data Protection Laws.

9.12 “**Service**” means the applicable service provided by Provider to Customer, as described in the Service Details.

9.13 “**Service Details**” means the description of the Service, information pertaining to the Processing of Customer Personal Data in connection with such Service, and other relevant details specific to the Service, if applicable, that are included in an appendix document titled “SERVICE DETAILS,” which is included with the relevant service contract or order forms as part of the Agreement.

9.14 “**Sub-processor**” means any person or entity engaged by Provider to Process Customer Personal Data.

EXHIBIT 1

TECHNICAL AND ORGANIZATIONAL MEASURES

Provider will implement and maintain commercially reasonable administrative, technical, and physical safeguards, including procedures and practices commensurate with the level of sensitivity of the Customer Personal Data and the nature of its activities under the Agreement, designed to protect the security, confidentiality, and integrity of Customer Personal Data Processed by Provider or in its possession and control.

The detailed list of the technical and organizational measures that Provider employs as part of its information security practices applicable to Provider-managed information technology systems is specified in the Service Details. The Parties acknowledge that data security requirements and risks are constantly changing, and therefore, Provider reserves the right to update such measures from time to time, provided that the updated measures will not materially decrease the overall level of protection of Customer Personal Data. For the avoidance of doubt, Provider's obligations under this Exhibit 1 to the DPA are limited to Customer Personal Data Processed by Provider on behalf of Customer.

EXHIBIT 2

TRANSFERS TO THIRD COUNTRIES

For the purpose of Exhibit 2, the “data exporter” or “Exporter” is Customer and the “data importer” or “Importer” is Provider.

PART I: Data Transfers Under Data Protection Laws that Recognize the 2021 EU Standard Contractual Clauses for International Transfers approved by the European Commission (“**EU SCC**s”)

The Parties agree to abide by the EU SCCs, which are recognized as a Valid Mechanism of international data transfers by the GDPR and substantially recognized by similar Data Protection Laws of certain Limited Transfer Regions. To the extent Provider is Processing Customer Personal Data subject to the GDPR or such other Data Protection Laws, the Parties hereby enter into the EU SCCs, which are hereby incorporated by reference, with the selected modules and options completed as set forth below.

1 EU SCCs

1.1 Clarifications of Definitions & Terms

A. For Limited Transfer Regions other than the European Economic Area, references to the GDPR or EU or Member State Law will be replaced by references to Data Protection Laws of the respective Limited Transfer Region.

B. The information to be listed in Annex I (A) and (B) of the APPENDIX of the EU SCCs, in addition to the identities of the data exporter and data importer as set forth above, are collectively listed in the Agreement, the DPA, and the Service Details.

C. All terms and definitions of the EU SCCs, whether or not capitalized or in quotes, are incorporated by reference into this Part I of Exhibit 2 to the DPA, notwithstanding any contrary definitions in other portions of the DPA.

1.2 Applicable Modules

With respect to Processing of Customer Personal Data:

A. When Customer is a Controller, and Provider is a Controller, Module One (transfer controller to controller) shall apply.

B. When Customer is a Controller, and Provider is a Processor, Module Two (transfer controller to processor) shall apply.

C. When Customer is a Processor, and Provider is a Sub-processor, Module Three (transfer processor to processor) shall apply.

1.3 Selected Options for EU SCCs

A. Optional Clause 7 (“Docking clause”) will be deemed incorporated.

B. In Clause 9 for Modules Two and Three, “Option 2: General Written Authorization” is selected, and the time period for prior notice of addition or replacement of Sub-processors will be as set forth in the DPA.

C. In Clause 11, the optional language will not apply.

D. With respect to Clause 12, the Parties agree that, solely as between the Parties, the limitations on liability negotiated between the Parties in the Agreement, if any, shall apply in connection with Clause 12, so long as they do not prejudice the rights or remedies of Data Subjects.

E. In Clause 17, for Module One, the Parties agree that the EU SCCs will be governed by the law of Ireland, except with respect to Limited Transfer Regions that do not accept such governing law, in which case the EU SCCs will be governed by the laws of such Limited Transfer Region.

F. In Clause 17, for Modules Two and Three, Option 2 is selected, and where the law of the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, the EU SCCs will be governed by the law of Ireland, except with respect to Limited Transfer

Regions that do not accept the governance by the law of a Member State, in which case the EU SCCs will be governed by the laws of such Limited Transfer Region.

G. In Clause 18(b), for Modules One, Two and Three, disputes will be resolved before the courts competent for the situs where the data exporter is established, and where the law of the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, before the competent courts of Ireland, except with respect to any Limited Transfer Regions that do not accept such courts as the chosen forum, where applicable, in which case disputes will be resolved before the courts of such jurisdictions.

H. The data protection supervisory authority for the situs where the data exporter is established is the competent authority, unless the transfer of such Limited Transfer Data is exclusively subject to the jurisdiction of another supervisory authority, where such supervisory authority shall accordingly be the competent supervisory authority.

I. The information required by Annex II of the APPENDIX of the EU SCCs is set forth in Exhibit 1 of this DPA.

J. The information required by Annex III of the APPENDIX of the EU SCCs is set forth in the Service Details.

K. By entering into the DPA, the Parties are deemed to be signing the EU SCCs, to the extent Provider's Processing of Customer Personal Data or transfer of Limited Transfer Data is subject to the GDPR.

2 **Data Exported from the United Kingdom of Great Britain and Northern Ireland ("UK")**. The UK's International Data Transfer Addendum to the EU SCCs ("UK IDTA") will be deemed incorporated into this DPA with respect to Personal Data exported from the UK that is subject to applicable Data Protection Laws in the UK, and the Parties confirm that the information required for the purposes of the UK IDTA is hereby completed as follows:

A. For Table 1 (Parties): the Parties' fields will be deemed to be pre-populated with the information respectively of Customer and Provider as set out in the Agreement.

B. For Table 2 (Selected SCCs, Modules and Selected Clauses): the applicable module of the SCCs including the Appendix Information and with only the modules, clauses or optional provisions listed in Sections 2 and 3 above will be brought into effect for the purpose of the UK SCCs.

C. For Table 3 (Appendix Information): the Appendix Information is set out in the following:

i. Annex 1A: List of Parties: as set out above and in the Agreement;

ii. Annex 1B: Description of Transfer: as set out in the Service Details;

iii. Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: as set out in Exhibit 1 of the DPA;

iv. Annex III: List of Sub processors: as set out in the Service Details with respect to Sub-processors.

D. For Table 4: the Parties agree that either Party may end the UK SCCs in accordance with the provisions of Section 19 of the UK SCCs.

E. For Part 2 "Mandatory Clauses": The clauses under the "Amendments to this Addendum" are hereby incorporated into the DPA except Clause 16, for which the amendment should be that (i) the Parties confirm that Clause 17 and/or 18 of the Addendum EU SCCs (as defined in the UK IDTA) shall refer to the laws and/or courts of England and Wales, (ii) a Data Subject may also bring legal proceedings against the (data) Exporter and/or Importer before any courts of the UK, and (iii) the Parties agree to submit themselves to the jurisdiction of such courts.

3 **Data Exported from Switzerland**. In case of any transfers of Personal Data from Switzerland subject to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), the Parties shall, as relevant and to the extent required by Swiss Data Protection Laws, (i) adopt the EU SCCs with the necessary

amendments under Swiss law, which will be deemed incorporated into the DPA. The EU SCCs shall be amended by including the following Appendix IV:

Appendix IV – Adaptions for Compliance with Swiss Law

In order for these Clauses to comply with Swiss law and thus be suitable for ensuring an adequate level of protection for data transfers from Switzerland to a third country in accordance with the Swiss Federal Act on Data Protection (**FADP**), these Clauses shall be amended with the following prevailing provisions.

3.1 The Parties adopt the standard of the Regulation (EU) 2016/679 for all data transfers.

3.2 Competent supervisory authority (EU SCCs Clause 13 / Annex I.C): To the extent the transfer of personal data as specified in Appendix A – Service Details (corresponding to EU SCCs Annex I.B) is governed by the FADP, the Swiss Federal Data Protection and Information Commissioner (FDPIC) shall act as the competent supervisory authority.

3.3 Governing law (Clause 17): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established, and where the law of the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, the EU SCCs will be governed by the law of Ireland, except with respect to Limited Transfer Regions that do not accept the governance by the law of Ireland, in which case the EU SCCs will be governed by the laws of such Limited Transfer Region.

3.4 Choice of forum and jurisdiction (Clause 18.a/b): Any dispute arising from these Clauses shall be resolved by the courts where the data exporter is established, except with respect to any Limited Transfer Regions that do not accept these courts (or the courts of Ireland, as applicable) as the chosen forum, where applicable, in which case disputes will be resolved before the courts of such Limited Transfer Region.

3.5 The term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of pursuing their rights at their place of habitual residence (Switzerland) in accordance with Clause 18.c. Accordingly, for Data Subjects habitually residing in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

PART II: Data Transfers Under Data Protection Laws with Requirements Different from or in Addition to the GDPR

1. Brazil

1.1 In relation to Limited Transfer Data transferred outside of Brazil, the Parties shall comply with Data Protection Laws and, unless either Party explicitly objects to the other Party, whenever applicable and legally required, adopt the standard contractual clauses as approved by the Brazilian data authority ("BR SCCs"), which are expressly incorporated herein by reference. The BR SCCs are hereby completed as follows:

A. Clause 1.1: The Parties are identified in the Agreement, the DPA, and the Service Details.
B. Clause 2.1: The description of the international transfer is set out in the Service Details
C. Clause 3.1: Option B shall apply, and the conditions of onward transfer are set out in Exhibit 1 of this DPA and in the Service Details.
D. Clause 4.1: "Option A" shall apply for transfers where Customer acts as Controller, and items a, b and c shall be the responsibility of Customer. "Option B" shall apply where Customer acts as Processor, items a, b and c shall be the responsibility of the Third-Party Controller, and where applicable, Third Party Controller information is set forth in the Service Details.
E. Section III: Details of security measures are set forth in Exhibit 1 to this DPA.

1.2 The BR SCCs shall be automatically updated, amended, replaced**,** or superseded from time to time in accordance with further instructions of the Brazilian data authority.

2. Canada

2.1 In relation to Limited Transfer Data subject to laws of Canada, to ensure the level of data protection required by applicable laws of Canada, the Parties shall comply with the Personal Information Protection and Electronic Documents Act (PIPEDA) and any other applicable laws on the federal, provincial, and territorial level of Canada. The Parties agree to abide by the principles established in PIPEDA, including (i) accountability/compliance with the principles, (ii) identification of the purposes/reasons for collecting the personal information, (iii) consent to the collection of the personal information, (iv) limiting the collection to only what is necessary in order to achieve the desired tasks, (v) limiting the use, disclosure and retention of the personal information, (vi) maintaining accurate data, (vii) safeguarding data with appropriate security policies, and (viii) making policies easily available to employees and customers. The data exporter shall notify individuals according to applicable laws, including but not limited that their personal data may be transferred outside of Canada and accordingly may be subject to access by foreign governments, courts, law enforcement or regulatory agencies.

2.2 In relation to Limited Transfer Data originating from the province of Québec, Canada, or otherwise subject to the Québec *Act respecting the protection of personal information in the private sector* (the "Québec Private Sector Act"), the following provisions shall apply:

A. The Parties shall comply with the Québec Private Sector Act and any other applicable laws of the province of Québec relating to privacy and the protection of personal data.
B. The Provider shall only use the Limited Transfer Data for the purposes of providing services to the Customer as provided for in the underlying service agreement between the Parties.
C. The Provider shall notify the Customer's person in charge of the protection of personal information of any violation or attempted violation by any person of any obligation concerning the confidentiality of the Limited Transfer Data.
D. The Provider shall allow the Customer's person in charge of personal information to conduct any verification relating to confidentiality requirements.
E. The Customer shall ensure that all Limited Transfer Data has been lawfully collected in compliance with the Québec Private Sector Act, and that the clear, free and informed consent of all persons concerned was duly obtained at the time of collection.
F. The Customer shall ensure that all Data Subjects concerned by the Limited Transfer Data have been duly notified, at the time of collection, that their personal information could be communicated outside the province of Québec.
G. The Customer has, prior to transferring the Limited Transfer Data, conducted an assessment of privacy-related factors compliant with the requirements of Québec law, including, without limitation, Section 17 of the Québec Private Sector Act, which assessment takes into account i) the sensitivity of the Limited Transfer Data, ii) the purposes for which the Limited Transfer Data will be used, iii) the protections (legal, contractual or otherwise) that will be afforded to the Limited Transfer Data, and iv) the privacy and data protection laws of the jurisdictions to which the Limited Transfer Data will be transferred, and that it is satisfied that the Limited Transfer Data will receive an adequate level of protection after the transfer is completed with regards to the requirements of the Québec Private Sector Act and generally recognized principles regarding the protection of personal information.
H. To the extent required to ensure that the Limited Transfer Data will receive an adequate level of protection within the meaning of the Québec Private Sector Act, the Parties agree to implement, in a written agreement, the terms necessary to mitigate any risks identified in the assessment of privacy-related factors referred to in paragraph G above.

3. South Korea

In relation to Limited Transfer Data transferred out of South Korea, if legally required, Customer shall secure grounds for the overseas transfer of personal information under the Personal Information Protection Act of Korea, such as obtaining the Data Subjects' consent for the data transfer, as applicable.

4. China

In relation to Limited Transfer Data transferred outside China, the Parties shall, as relevant and to the extent required by Chinese Data Protection Law, (i) adopt the Standard Contract approved by the Cyberspace Administration of China ("CAC"), which will be deemed to supplement (and take precedence over) the DPA and shall be read and interpreted in the light of the provisions and definitions of applicable laws, (ii) pass the CAC's data transfer security assessment as required by law, or (iii) obtain the data transfer certification as approved by the CAC. Where the data transfer requires consent of Data Subjects, Customer shall ensure such consent of Data Subjects is in place as legally required.

5. Singapore

In relation to Limited Transfer Data transferred outside Singapore, as relevant and to the extent required by Singapore’s Personal Data Protection Act (2012) and its regulations in force (“PDPA”), to which the EU SCCs do not apply, the provisions of the main body of this DPA shall apply to such transfer to ensure a comparable standard of protection of the Limited Transfer Data as provided under the PDPA, and (i) the Parties shall ensure that the Limited Transfer Data is accurate and up to date, and (ii) Customer shall secure grounds for the transfer of Limited Transfer Data under the PDPA, including without limitation obtaining the deemed or express consent of the Data Subjects as applicable.

6. Other Mandatory Standard Clauses

To the extent any other Limited Transfer Region does not recognize the EU SCCs and adopts other standard clauses that are mandatory for transfers of Personal Data from such Limited Transfer Region, unless either Party explicitly objects to the other Party, the Parties agree that such clauses will be deemed incorporated into this DPA with respect to Personal Data from such Limited Transfer Region, and relevant details of the Agreement, including but not limited to the DPA and Service Details, will be used to complete the information required by such clauses.

The competent supervisory authority should be decided in accordance with Data Protection Laws; in absence of clear legal guidance, it should be the authority of the jurisdiction where the headquarters of Customer resides.

EXHIBIT 3

CALIFORNIA CONSUMER PRIVACY ACT ADDENDUM

(“**CCPA Addendum**”)

This CCPA Addendum shall apply with respect to Customer Personal Data that is subject to the CCPA and Processed by Provider on behalf of Customer (“California Personal Information”).

The terms used in this CCPA Addendum shall have the meanings set forth in this CCPA Addendum, and capitalized terms not otherwise defined herein shall have the meanings given to them in the remainder of the DPA.

Where Customer acts as the “business” and Provider acts as the “service provider” or “contractor” to Customer, as defined under the CCPA, the following provisions shall apply.

1. Customer shall disclose California Personal Information to Provider for the limited and specific business purposes set forth in the Agreement, Service Details, and/or Service description, as applicable, or as otherwise permitted by the CCPA.

2. Provider shall comply with applicable obligations under the CCPA and provide the same level of protection to California Personal Information as required of Customer by the CCPA.

3. Provider shall not “sell” or “share” California Personal Information as those terms are defined in the CCPA.

4. Provider shall not retain, use, or disclose California Personal Information for any commercial or other purpose other than the business purpose(s) specified in the Agreement (including this DPA), nor otherwise Process California Personal Information outside the direct business relationship with Customer, unless otherwise permitted by the CCPA or required by law. Provider shall not combine California Personal Information that it receives from Customer pursuant to this DPA or the Agreement, with California Personal Information that it receives from or on behalf of another person or collects from its own interaction with a California resident, subject to any exceptions set forth in the CCPA.

5. Customer may take reasonable and appropriate steps to ensure that Provider uses California Personal Information in a manner consistent with the Customer’s obligations under the CCPA, and upon notice, to stop and remediate any unauthorized use of California Personal Information by Provider.

6. Customer shall inform Provider of any consumer request made pursuant to the CCPA that Provider must comply with and provide the information necessary for Provider to comply with the request (or Provider may enable the Customer to comply with consumer requests directly should such functionality be available as part of the Service).

7. If Provider determines it can no longer meet its obligations under the CCPA, it shall promptly notify Customer.

8. To the extent that the Parties Process “deidentified” information as that term defined in the CCPA, each Party shall (a) take reasonable measures to ensure that the information cannot be associated with a consumer or household, (b) commit to maintaining and using the information in deidentified form and not to attempt to reidentify the information, except that a Party may attempt to reidentify the information for the purpose of determining whether its deidentification processes satisfy the requirements of CCPA, and (c) contractually obligate any recipients of the information to comply with these restrictions.

9. To the extent Provider is a contractor, it certifies that it understands the restrictions in set forth above and will comply with them.