CUSTOMER AGREEMENT

This Customer Agreement (SaaS) (this **"Agreement"**) is between UNIFYAPPS Inc., a Delaware corporation (**"UnifyApps"**), and the entity identified as 'Customer' in the Order Form ("**Order Form #1**") attached at the cover of this Agreement ("**Customer**" or "**Client**"), and is effective as of the date of execution of the Order Form 1 (the **"Effective Date"**).

Background

UnifyApps has developed and makes software as a service available, comprising Unify Agentic AI, Unify Applications, Unify Automations, Unify Data collectively known as the **"UnifyApps Product"**.

1. Definitions

1.1 The following terms, when used in this Agreement will have the following meanings:

"Affiliates" means an entity that directly or indirectly Controls, is Controlled by, or is under common Control with another entity, so long as such Control exists. For the purposes of this definition, **"Control"** means beneficial ownership of 50% or more of the voting power or equity in an entity.

"Confidential Information" means any information or data disclosed by either party that is marked or otherwise designated as confidential or proprietary or that should otherwise be reasonably understood to be confidential in light of the nature of the information and the circumstances surrounding disclosure. However, "Confidential Information" will not include any information which (a) is in the public domain through no fault of receiving party; (b) was properly known to receiving party, without restriction, prior to disclosure by the disclosing party; (c) was properly disclosed to receiving party, without restriction, by another person with the legal authority to do so; or (d) is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information.

"Documentation" means the printed and digital instructions, on-line help files, technical documentation and user manuals made available by UnifyApps for the UnifyApps Product.

"Intellectual Property Rights" means all current and future copyright, patents, trademarks or rights in fonts, databases, inventions or trade secrets, know-how, rights in designs, topographies, trade and business names, domain names, marks and devices (whether or not registered) and all other intellectual property rights and applications for any of those rights (where such applications can be made) capable of protection in any relevant country of the world.

"Non-UnifyApps Product" means a third party or Customer web-based, mobile, offline or other software application that integrates with the UnifyApps Product (other than third party data hosting services used by UnifyApps). For clarity, the UnifyApps Product excludes Non-UnifyApps Products.

"Order Form" means an order form, quote or other similar document that sets forth the specific UnifyApps Product and pricing therefore (including in relation to overages), permitted number of users and subscription term, and that references this Agreement and is mutually executed by the parties. In case of any inconsistency between the terms of this Agreement and Order Form, the terms mentioned in this Agreement shall prevail unless specifically agreed in the Order Form. Order Form #1 is attached hereto as the cover of this Agreement and has been mutually executed as of the Effective Date, subject to the terms of this Agreement.

"**SLA**" means UnifyApps' Service Level Agreement, located here, and as may be updated by UnifyApps from time to time, which is incorporated herein by reference and forms an integral part hereof.

"UnifyApps IP" means all work product, improvements, developments, discoveries, proprietary information, trademarks, copyrights, trade names, logos, art work, slogans, know-how, processes, methods, trade secrets, source code, application development, designs, drawings, plans, business plans or models, blue prints (whether or not

registrable and whether or not design rights subsist in them), utility models, works in which copyright may subsist (including computer software and preparatory and design materials thereof), inventions (whether patentable or not, and whether or not patent protection has been applied for or granted) and all other intellectual property throughout the world, in and for all languages, including but not limited to computer and human language; owned and/or developed by UnifyApps and/or its Affiliates, including in connection with the proprietary technology of UnifyApps, UnifyApps Product, Documentation, and any derivatives, improvements, enhancements or extensions of such technology conceived, reduced to practice or developed.

2. UnifyApps Product

2.1 Provision of UnifyApps Product. Subject to the terms and conditions of this Agreement, UnifyApps will make the UnifyApps Product available to Customer pursuant to this Agreement, the SLA, and the applicable Order Form, and hereby grants Customer a non-exclusive and non-licensable or sublicensable, non-transferable, and revocable license to access and use the UnifyApps Product for its internal business purposes. The rights provided by UnifyApps to the Customer hereunder shall be subject to the Customer complying with its responsibilities as set forth herein, including under Section 2.3.

2.2 Data Security.

(a) UnifyApps will maintain a security program materially in accordance with industry standards that is designed to (i) ensure the security and integrity of Customer data uploaded by or on behalf of Customer to the UnifyApps Product (**"Customer Data"**); (ii) protect against threats or hazards to the security or integrity of Customer Data; and (iii) prevent unauthorized access to Customer Data.

(b) To the extent that UnifyApps processes any Personal Data (as defined in the DPA referenced below) contained in Customer Data that is subject to Data Protection Legislation (as defined in the DPA), on Customer's behalf, in the provision of the UnifyApps Product, the parties will execute a Data Processing Addendum (**"DPA"**) attached hereto as Annexure A, and such DPA is hereby deemed incorporated herein by reference.

2.3 Customer Responsibilities.

(a) Customer acknowledges that UnifyApps's provision of the UnifyApps Product is dependent on Customer providing all reasonably required cooperation (including the prompt provision of access to Customer's systems, personnel, cooperation and materials as reasonably required and any other access as may be specified in the applicable Order Form), and Customer will provide all such cooperation in a diligent and timely manner.

(b) Customer will (i) be responsible for all use of the UnifyApps Product under its account, (ii) use commercially reasonable efforts to prevent unauthorized access to or use of the UnifyApps Product and notify UnifyApps promptly of any such unauthorized access or use or any other known or suspected breach of security or misuse of the UnifyApps Product and (iii) be responsible for obtaining and maintaining any equipment, software and ancillary services needed to connect to, access or otherwise use the UnifyApps Product, including as set forth in the Documentation. Customer will be solely responsible for its failure to maintain such equipment, software and services, and UnifyApps will have no liability for such failure (including under any service level agreement).

(c) Customer will not use the UnifyApps Product to transmit or provide to UnifyApps any financial or medical information of any nature, or any sensitive personal data (e.g., social security numbers, driver's license numbers, birth dates, personal bank account numbers, passport or visa numbers and credit card numbers).

(d) Customer shall be responsible for the content of all communications sent by its users via the UnifyApps Product. Customer agrees that it will not use the UnifyApps Product to communicate any message or material that (i) is libellous, harmful to minors, obscene or constitutes pornography; (ii) infringes the intellectual property rights of any third party or is otherwise unlawful; or (iii) constitutes or encourages conduct that could constitute a criminal offense.

2.4 Affiliates. Any Affiliate of Customer will have the right to enter into an Order Form executed by such Affiliate and UnifyApps and this Agreement will apply to each such Order Form as if such Affiliate were a signatory to this Agreement. With respect to such Order Forms, such Affiliate becomes a party to this Agreement and references to Customer in this Agreement are deemed to be references to such Affiliate.

3. Fees

3.1 Fees. Customer will pay UnifyApps the fees set forth in the applicable Order Form. Customer shall pay those amounts due and not disputed in good faith within thirty (30) days of the date of receipt of the applicable invoice, unless a specific date for payment is set forth in such Order Form, in which case payment will be due on the date specified. Except as otherwise specified herein or in any applicable Order Form, (a) fees are quoted and payable in United States dollars and (b) payment obligations are non-cancelable and non-pro-ratable for partial months, and fees paid are non-refundable.

3.2 Late Payment. UnifyApps may suspend access to the UnifyApps Product immediately upon notice if Customer fails to pay any amounts hereunder at least five (5) days past the applicable due date. If UnifyApps has not received payment within five (5) days after the applicable due date, interest will accrue on past due amounts at the rate of one percent (1%) per month, but in no event greater than the highest rate of interest allowed by law, calculated from the date such amount was due until the date that payment is received by UnifyApps.

3.3 Taxes. All amounts payable hereunder are exclusive of any sales, use and other taxes or duties, however designated (collectively "Taxes"). Customer will be solely responsible for payment of all Taxes, except for those taxes based on the income of UnifyApps. Customer will not withhold any Taxes from any amounts due to UnifyApps.

4. Proprietary Rights

4.1 Proprietary Rights.

(a) As between the parties, UnifyApps exclusively owns all right, title and interest in and to the UnifyApps Product, UnifyApps IP, System Data and UnifyApps's Confidential Information (and Intellectual Property Rights in connection with each of the foregoing), and Customer exclusively owns all right, title and interest in and to its data, insights produced specifically for Customer via the use of the UnifyApps Product by Customer and Customer's Confidential Information. "**System Data**" means data collected by UnifyApps regarding the UnifyApps Product that may be used to generate logs, statistics or reports regarding the performance, availability, usage, integrity or security of the UnifyApps Product.

(b) To the extent that, by operation of law or otherwise, any UnifyApps IP and/or Intellectual Property Rights in relation thereto, are acquired or obtained by the Customer and/or any of its Affiliates, Customer hereby assigns, and shall procure that such Affiliates assign (including by way of present assignment of future rights) to (or will procure the assignment to), UnifyApps, with full title guarantee, absolutely and free from encumbrances and restrictions, any such UnifyApps IP and/or Intellectual Property Rights in relation thereto. At UnifyApps' request, the Customer agrees to execute documents or take other reasonable steps in order that UnifyApps may acquire, transfer, maintain, perfect, and enforce UnifyApps's rights set out herein.

4.2 Feedback. Customer may from time to time provide UnifyApps suggestions or comments for enhancements or improvements, new features or functionality or other feedback ("Feedback") with respect to the UnifyApps Product. UnifyApps will have full discretion to determine whether or not to proceed with the development of any requested enhancements, new features or functionality. UnifyApps will have the full, unencumbered right, without any obligation to compensate or reimburse Customer, to use, incorporate and otherwise fully exercise and exploit any such Feedback in connection with its products and services.

5. Confidentiality; Restrictions

5.1 Confidentiality. Each party agrees that it will use the Confidential Information of the other party solely in accordance with the provisions of this Agreement and it will not disclose the same directly or indirectly, to any third party without the other party's prior written consent, except as otherwise permitted hereunder. However, either party may disclose Confidential Information (a) to its employees, officers, directors, attorneys, auditors, financial advisors and other representatives who have a need to know and are legally bound to keep such information confidential by confidentiality obligations consistent with those of this Agreement; and (b) as required by law (in which case the receiving party will provide the disclosing party with prior written notification thereof, will provide the disclosing party with the opportunity to contest such disclosure, and will use its reasonable efforts to minimize such disclosure to the extent permitted by applicable law. Neither party will disclose the terms of this Agreement to any third party, except that either party may confidentially disclose such terms to actual or potential lenders, investors or acquirers. Each party agrees to exercise due care in protecting the Confidential Information from unauthorized use and disclosure. In the event of actual or threatened breach of the provisions of this Section 5, the non-breaching party will be entitled to seek immediate injunctive and other equitable relief, without waiving any other rights or remedies available to it. Each party will promptly notify the other in writing if it becomes aware of any violations of the confidentiality obligations set forth in this Agreement.

5.2 Technology Restrictions. Customer will not directly or indirectly: (a) reverse engineer, decompile, disassemble, modify, create derivative works of or otherwise create, attempt to create or derive, or permit or assist any third party to create or derive, the source code underlying the UnifyApps Product; (b) attempt to probe, scan or test the vulnerability of the UnifyApps Product, breach the security or authentication measures of the UnifyApps Product without proper authorization or wilfully render any part of the UnifyApps Product unusable; (c) use or access the UnifyApps Product to develop a product or service that is competitive with UnifyApps's products or Product or engage in competitive analysis or benchmarking; (d) transfer, distribute, resell, lease, license, or assign the UnifyApps Product or otherwise offer the UnifyApps Product on a standalone basis; or (e) otherwise use the UnifyApps Product in violation of applicable law (including any export law) or outside the scope expressly permitted hereunder and in the applicable Order Form.

6. Warranties and Disclaimers

6.1 UnifyApps. UnifyApps warrants that it will, consistent with prevailing industry standards, provide the UnifyApps Product in a professional and workmanlike manner and the UnifyApps Product will conform in all material respects with the Documentation. For material breach of the foregoing express warranty, Customer's exclusive remedy shall be the re-performance of the deficient UnifyApps Product or, if UnifyApps cannot re-perform such deficient UnifyApps Product as warranted within thirty (30) days after receipt of written notice of the warranty breach, Customer shall be entitled to terminate the applicable Order Form and recover a pro-rata portion of the prepaid subscription fees corresponding to the terminated portion of the applicable subscription term.

6.2 Customer. Customer warrants that it has all rights necessary to provide any information, data or other materials that it provides hereunder, and to permit UnifyApps to use the same as contemplated hereunder.

6.3 DISCLAIMERS. EXCEPT AS EXPRESSLY SET FORTH HEREIN, EACH PARTY DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

7. Indemnification

7.1 Indemnity by UnifyApps. UnifyApps will defend Customer against any claim, demand, suit, or proceeding ("Claim") made or brought against Customer by a third party alleging that the use of the UnifyApps Product as permitted hereunder infringes or misappropriates a United States patent, copyright or trade secret and will indemnify Customer for any damages finally awarded against Customer (or any settlement approved by UnifyApps) in connection with any such Claim; provided that (a) Customer will promptly notify UnifyApps of such Claim, (b) UnifyApps will have the sole and exclusive authority to defend and/or settle any such Claim (provided that UnifyApps may not settle any Claim without Customer's prior written consent, which will not be unreasonably withheld, unless it unconditionally releases Customer of all related liability) and (c) Customer reasonably cooperates with UnifyApps in connection therewith. If the use of the UnifyApps Product by Customer has become, or in UnifyApps's opinion is likely to become, the subject of any claim of infringement, UnifyApps may at its option and

expense (i) procure for Customer the right to continue using and receiving the UnifyApps Product as set forth hereunder; (ii) replace or modify the UnifyApps Product to make it non-infringing (with comparable functionality); or (iii) if the options in clauses (i) or (ii) are not reasonably practicable, terminate the applicable Order Form and provide a pro rata refund of any prepaid subscription fees corresponding to the terminated portion of the applicable subscription term. UnifyApps will have no liability or obligation with respect to any Claim if such Claim is caused in whole or in part by (A) compliance with designs, guidelines, plans or specifications provided by Customer; (B) use of the UnifyApps Product by Customer not in accordance with this Agreement; (C) modification of the UnifyApps Product by or on behalf of Customer; (D) Customer Confidential Information or (E) the combination, operation or use of the UnifyApps Product with other products or services where the UnifyApps Product would not by itself be infringing (clauses (A) through (E), "Excluded Claims"). This Section states UnifyApps's sole and exclusive liability and obligation, and Customer's exclusive remedy, for any claim of any nature related to infringement or misappropriation of intellectual property.

7.2 Indemnification by Customer. Customer will defend UnifyApps against any Claim made or brought against UnifyApps by a third party arising out of the Excluded Claims, and Customer will indemnify UnifyApps for any damages finally awarded against UnifyApps (or any settlement approved by Customer) in connection with any such Claim; provided that (a) UnifyApps will promptly notify Customer of such Claim, (b) Customer will have the sole and exclusive authority to defend and/or settle any such Claim (provided that Customer may not settle any Claim without UnifyApps's prior written consent, which will not be unreasonably withheld, unless it unconditionally releases UnifyApps of all liability) and (c) UnifyApps reasonably cooperates with Customer in connection therewith.

8. Limitation of Liability

EXCEPT FOR A PARTY'S BREACH OF SECTION 5 OR A PARTY'S INFRINGEMENT OR MISAPPROPRIATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS,UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, WILL EITHER PARTY BE LIABLE TO THE OTHER UNDER THIS AGREEMENT FOR (A) ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY CHARACTER, INCLUDING DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOST SALES OR BUSINESS, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOST CONTENT OR DATA, EVEN IF A REPRESENTATIVE OF SUCH PARTY HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES, OR (B) EXCLUDING CUSTOMER'S PAYMENT OBLIGATIONS, ANY AGGREGATE DAMAGES, COSTS, OR LIABILITIES IN EXCESS OF THE AMOUNTS PAID BY CUSTOMER UNDER THE APPLICABLE ORDER FORM DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM.

9. Termination

9.1 **Term**. The term of this Agreement will commence on the Effective Date and continue until terminated as set forth below. The initial term of each Order Form will begin on the Order Form Effective Date of such Order Form and will continue for the subscription term set forth therein. Except as set forth in such Order Form, the term of such Order Form will automatically renew for successive renewal terms equal to the length of the initial term of such Order Form, unless either party provides the other party with written notice of non-renewal at least thirty (30) days prior to the end of the then-current term.

9.2 **Termination**. Each party may terminate this Agreement upon written notice to the other party if there are no Order Forms then in effect. Each party may also terminate this Agreement or the applicable Order Form upon written notice in the event (a) the other party commits any material breach of this Agreement or the applicable Order Form and fails to remedy such breach within thirty (30) days after written notice of such breach or (b) subject to applicable law, upon the other party's liquidation, commencement of dissolution proceedings or assignment of substantially all its assets for the benefit of creditors, or if the other party become the subject of bankruptcy or similar proceeding that is not dismissed within sixty (60) days.

9.3 **Survival**. Upon expiration or termination of this Agreement all rights and obligations will immediately terminate except that any terms or conditions that by their nature should survive such expiration or termination will survive, including the License Restrictions and terms and conditions relating to proprietary rights/Intellectual

Property Rights and confidentiality, technology restrictions, disclaimers, indemnification, limitations of liability and termination and the general provisions below. Upon expiration or termination of this Agreement, each party will return or destroy, at the other party's option, any Confidential Information of such party in the other party's possession or control.

9.4 Customer Data Retrieval. Upon Customer's written request made on or prior to expiration or termination of the applicable Order Form, UnifyApps will give Customer limited access to the UnifyApps Product for a period of up to thirty (30) days after such expiration or termination, at no additional cost, solely for purposes of retrieving Customer Data. Subject to such retrieval period and UnifyApps's legal obligations, UnifyApps has no obligation to maintain or provide any Customer Data and will, unless legally prohibited, delete Customer Data after such expiration or termination; provided, however, that UnifyApps will not be required to remove copies of the Customer Data from its backup media and servers until such time as the backup copies are scheduled to be deleted, provided further that in all cases UnifyApps will continue to protect the Customer Data in accordance with this Agreement. For clarity, during the term of the applicable Order Form, Customer may extract Customer Data using UnifyApps's standard web services as described in the Documentation.

10. General

10.1 Publicity. Customer agrees that UnifyApps may refer to and utilize Customer's name and trademarks in UnifyApps's marketing materials, website, events, and other publicity materials and activities (such as press releases, testimonials, customer references, and case studies).

10.2 Assignment; Delegation. Neither party hereto may assign or otherwise transfer this Agreement, in whole or in part, without the other party's prior written consent, except that (i) either party may assign this Agreement without consent to a successor to all or substantially all of its assets or business related to this Agreement, and/or (ii) UnifyApps may assign this Agreement to any of its Affiliates. Any attempted assignment, delegation, or transfer by either party in violation hereof will be null and void. Subject to the foregoing, this Agreement will be binding on the parties and their successors and assigns.

10.3 Amendment; Waiver. No amendment or modification to this Agreement and/or any Order Form, nor any waiver of any rights hereunder or thereunder, will be effective unless assented to in writing by both parties. Any such waiver will be only to the specific provision and under the specific circumstances for which it was given, and will not apply with respect to any repeated or continued violation of the same provision or any other provision. Failure or delay by either party to enforce any provision of this Agreement will not be deemed a waiver of future enforcement of that or any other provision.

10.4 Relationship. Nothing contained herein will in any way constitute any association, partnership, agency, employment or joint venture between the parties hereto, or be construed to evidence the intention of the parties to establish any such relationship. Neither party will have the authority to obligate or bind the other in any manner, and nothing herein contained will give rise or is intended to give rise to any rights of any kind to any third parties.

10.5 Unenforceability. If a court of competent jurisdiction determines that any provision of this Agreement is invalid, illegal, or otherwise unenforceable, such provision will be enforced as nearly as possible in accordance with the stated intention of the parties, while the remainder of this Agreement will remain in full force and effect and bind the parties according to its terms.

10.6 Governing Law. This Agreement will be governed by the laws of the State of New York, exclusive of its rules governing choice of law and conflict of laws. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods.

10.7 Notices. Any notice required or permitted to be given hereunder will be given in writing by personal delivery, certified mail, return receipt requested, or by overnight delivery. Notices to the parties must be sent to the respective address set forth in the **"Order Form"**, or such other address designated pursuant to this Section.

10.8 Entire Agreement. This Agreement (read with the Order Forms, which shall be deemed to be included in any and all references to 'Agreement' hereunder) comprises the entire agreement between Customer and UnifyApps with respect to its subject matter, and supersedes all prior and contemporaneous proposals, statements, sales materials or presentations and agreements (oral and written). No oral or written information or advice given by UnifyApps, its agents or employees will create a warranty or in any way increase the scope of the warranties in this Agreement.

10.9 Force Majeure. Neither Party will be deemed in breach hereunder for any cessation, interruption or delay in the performance of its obligations due to causes beyond its reasonable control ("Force Majeure Event"), including earthquake, flood, or other natural disaster, act of God, labor controversy, civil disturbance, terrorism, war (whether or not officially declared), cyber attacks (e.g., denial of service attacks), or the inability to obtain sufficient supplies, transportation, or other essential commodity or service required in the conduct of its business, or any change in or the adoption of any law, regulation, judgment or decree.

10.10 Government Terms. UnifyApps provides the UnifyApps Product, including related software and technology, for ultimate federal government end use solely in accordance with the terms of this Agreement. If Customer is an agency, department, or other entity of any government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the UnifyApps Product, or any related documentation of any kind, including technical data, software, and manuals, is restricted by the terms of this Agreement. All other use is prohibited and no rights than those provided in this Agreement are conferred. The UnifyApps Product was developed fully at private expense.

10.11 Interpretation. For purposes hereof, "including" means "including without limitation".

[Remainder of Page Intentionally Left Blank]

Annexure A

Data Processing Addendum

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this DPA.

1.3 "Company Account Data" means personal data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.4 "Company Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.5 "Data Exporter" means Customer.

1.6 "Data Importer" means Company.

1.7 "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including, each as applicable: (i) the Information Technology Act, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, and the Digital Personal Data Protection Act, 2023 and rules and regulations under each of the foregoing, (ii) the California Consumer Privacy Act ("CCPA") and similar U.S. state consumer privacy laws, (iii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (iv) the Swiss Federal Act on Data Protection; (v) the UK Data Protection Act 2018; and (vi) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the GDPR.

1.8 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic

Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.9 "ex-UK Transfer" means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data

Importer (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.10"Services" shall have the meaning set forth in the Agreement.

1.11 "Standard Contractual Clauses" means (i) the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "EU SCCs"), and (ii) where the UK GDPR applies, the EU SCCs as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018 (the "UK SCCs").

2. Relationship of the Parties; Processing of Data

2.1 The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data.

2.2 Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

2.4 Following completion of the Services, at Customer's choice, Company shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (if applicable) shall be provided by Company to Customer only upon Customer's request.

2.5 CCPA. Except with respect to Company Account Data and Company Usage Data, the parties acknowledge and agree that Company is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving Personal Data from Customer in order to provide the Services pursuant to the Agreement, which constitutes a business purpose. Company shall not "sell" or "share" any such Personal Data. Company shall not retain, use or disclose any Personal Data provided by Customer pursuant to the Agreement, or combine such Personal Data with Personal Data Company has collected from any other source, except as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. The terms "business purpose," "service provider," "sell," and "share" are as defined in Section 1798.140 of the CCPA. Company certifies that it understands the restrictions of this Section 2.5.

3. Confidentiality

3.1 Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Authorized Sub-Processors

4.1 Customer acknowledges and agrees that Company may (1) engage its Affiliates as well as the Authorized Sub-Processors on the List (defined below) to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this DPA, Customer provides general written authorization to Company to engage sub-processors as necessary to perform the Services.

4.2 A list of Company's current Authorized Sub-Processors (the "List") is available to Customer at Sub-processors Link. Such List may be updated by Company from time to time. Company will provide a mechanism to subscribe to notifications (which may include but are not limited to email notifications) of new Authorized Sub-Processors and Customer, if it wishes, will subscribe to such notifications where available. If Customer does not subscribe to such notifications, Customer waives any right it may have to receive prior notice of changes to Authorized Sub-Processors. At least ten (10) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Company will add such third party to the List and notify subscribers, including Customer, via the aforementioned notifications. Customer may object to such an engagement by informing Company in writing within ten (10) days of receipt of the aforementioned notice by Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Company from offering the Services to Customer.

4.3 If Customer reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

4.4 If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

4.5 Company will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

4.6 If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Company to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Company beforehand, and that such copies will be provided by the Company only upon request by Customer.

5. Security of Personal Data.

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information about the Company's technical and organizational security measures.

6. Transfers of Personal Data

6.1 The parties agree that the Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary

processing operations take place in India, and that the transfer of Customer's Personal Data to India is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows, to the extent applicable:

6.2.1 Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 9 of this DPA.

6.2.2 Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.

6.2.3 Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Company is processing Personal Data on behalf of Customer as a sub-processor.

6.3 For each module, where applicable the following applies:

6.3.1 The optional docking clause in Clause 7 does not apply.

6.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this DPA;

6.3.3 In Clause 11, the optional language does not apply;

6.3.4 All square brackets in Clause 13 are hereby removed;

6.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by Ireland law.

6.3.6 In Clause 18(b), disputes will be resolved before the courts of Ireland;

6.3.7 Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs;

6.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs; and

6.3.9 By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

6.4 Ex-UK Transfers. The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as Exhibit D of this DPA.

6.5 Transfers from Switzerland. The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

6.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

6.5.2 The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

6.5.3 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

6.5.4 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.6 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

6.6.1 As of the date of this DPA, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests")**;**

6.6.2 If, after the date of this DPA, the Data Importer receives any Government Agency Requests, Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of the such Government Agency Requests; and

6.6.3 The Data Exporter and Data Importer will meet as needed to consider whether:

(i) the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

(ii) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

(iii) it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

6.6.4 If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

6.6.5 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

7. Rights of Data Subjects

7.1 Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal

Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

7.2 Company shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8. Actions and Access Requests; Audits

8.1 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under Data Protection Laws, including to provide information to Customer to assist Customer with any required data protection impact assessment and/or to demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.2 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the Data Protection Laws. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.3 Data is stored for a period as specified by the contractual obligations with the customer. Additionally retention policies are determined by the customer based on their specific needs such as operational purposes, compliance, applicable laws or business use. Customer shall, with reasonable notice to Company, have the right to review, audit and copy such records at Company's offices during regular business hours.

8.4 Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8.4.

8.5 Company shall immediately notify Customer if an instruction, in the Company's opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6 In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

8.7 In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8 The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.6 and 8.7 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. Company's Role as a Controller. The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process Company Account Data and Company Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Company may also process Company Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by the Company as a controller shall be in accordance with the Company's privacy policy set forth at https://www.unifyapps.com/privacy-policy**.**

10. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the Company's Privacy Policy (2) the applicable terms in the Standard Contractual Clauses; (3) the Agreement; and (4) the terms of this DPA. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

11. Execution of this DPA. Company has pre-signed this DPA, in the signature block below and in each of the main body, and Exhibit B (as the "data importer"). To complete this DPA, Customer must: (i) complete the information requested in the signature block below and sign there, (ii) complete the information requested of the "data exporter" on Exhibits B, and (iii) send the completed and signed Addendum to Company by email to legal@unifyapps.com. Upon receipt of the validly completed Addendum by Company at this email address, this DPA will become legally binding.

Customer	**UNIFYAPPS INC.**
Signature: **Customer Legal Name:**	**Signature:**
Print Name:	**Print Name:**
Title:	**Title:**
Date:	**Date:**

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Protecting data, including restricting, encrypting, and security testing
- Holding data, including storage, organization, and structuring
- Erasing data, including destruction and deletion
- Analyzing data, including product usage assessment
- Sharing data, including disclosure to sub processors as permitted in this DPA

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Company Account Data and Company Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects: Customer's employees, consultants, contractors, and/or agents.

Categories of Personal Data: Company processes Personal Data contained in Company Account Data, Company Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include name, email, job title, username, Company device identifiers (e.g. serial number), IP address for company device, installed applications for company device, background check verification records (at discretion of Controller), security training records.

Sensitive Data or Special Categories of Data: Customers are prohibited from providing sensitive personal data or special categories of data to Company, including without limitation, any data which discloses the criminal history.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

Data exporter(s):

Name:

Trading Name (if different):

Address: ;

Official Registration Number (if any) (company number or similar identifier):

Contact person's name, position and contact details: , ,

Activities relevant to the data transferred under these Clauses: As described in Section 2 of the DPA.

Signature and date:

Role (controller/processor): Controller

Data importer(s):

Name: UNIFYAPPS INC.

Address and contact information: UnifyApps, Inc., WeWork, 575 5th Ave, New York, NY 10017, USA

Official Registration Number : 20233820672

Activities relevant to the data transferred under these Clauses: As described in Section 2 of the DPA.

Signature and date:

Role (controller/processor): As described in Section 2 of the DPA.

2. Description of the Transfer

Data Subjects	As described in Exhibit A of the DPA
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA

Recipients of Personal Data Transferred to the Data Importer	Company will maintain a list of Authorized Sub-Processors.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

Exhibit C

Description of the Technical and Organizational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum.

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest. Company uses only recommended secure cipher suites and protocols to encrypt all traffic in transit and Customer Data is securely encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Company's customer agreements contain strict confidentiality obligations. Additionally, Company requires every downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in Company's customer agreements. Company is SOC 2 Type I and Type II compliant and includes the Security and Processing Integrity Trust Service Criteria.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Daily backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Company is SOC 2 Type I and Type II compliant and includes the Security and Processing Integrity Trust Service Criteria.
Measures for user identification and authorization	Company uses secure access protocols and processes and follows industry best-practices for authentication, including Multifactor Authentication and Single Sign On (SSO). All production access requires the use of VPN or two-factor authentication, and network infrastructure is securely configured to vendor and industry best practices to block all unnecessary ports, services, and unauthorized network traffic.
Measures for the protection of data during transmission	All the communication between services and service to database is protected using TLS 1.2. All databases have TLS enabled and Linkerd is used for service to service communication which has TLS enabled. All managed services like Kafka (MSK), AWS Memory db, AWS Document DB also have TLS enabled to ensure encryption in transit. All load balancer traffic coming on HTTP is redirected to HTTPS automatically to ensure secure communication.

Measures for the protection of data during storage	All database and application pod disks are encrypted using AWS KMS key using AES encryption which ensures all critical data is encrypted at rest. Data is encrypted by using AES 256 encryption key.
Measures for ensuring physical security of locations at which personal data are processed	All Company processing occurs in physical data centers that are managed by AWS. https://aws.amazon.com/compliance/data-center/controls/
Measures for ensuring events logging	Company monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Company adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	Company is ISO/IEC 27001:2022, ISO 27701:2019, GDPR and SOC2 Type I and Type II compliant. The framework for the Company's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.
Measures for certification/assurance of processes and products	Company is ISO/IEC 27001:2022, ISO 27701:2019, GDPR and SOC2 Type I and Type II compliant. The framework for the Company's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.
Measures for ensuring data minimisation	Company's Customers unilaterally determine what data they route through the Services. As such, Company operates on a shared responsibility model. Company gives Customers control over exactly what data enters the platform. Additionally, the Company has built in self-service functionality to the Services that allows Customers to delete and suppress data at their discretion.
Measures for ensuring data quality	Company has a multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) We are using Rest with OpenAPI Specification and have tools around to ensure strict contracts. Company applies these measures across the board, both to ensure the quality of any Usage Data that Company collects and to ensure that the Company Platform is operating within expected parameters. Company ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data is presented or exported.

Measures for ensuring limited data retention	Customers unilaterally determine what data they route through the Services. As such, Company operates on a shared responsibility model. If a Customer is unable to delete Personal Data via the self-services functionality of the Services, then the Company deletes such Personal Data upon the Customer's written request, within the timeframe specified in this DPA and in accordance with Applicable Data Protection Law. All Personal Data is deleted from the Services following service termination.
Measures for ensuring accountability	Company has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Personal Data Breaches, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, the Company conducts regular third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	Personal Data submitted to the Services by Customer may be deleted by the Customer or at the Customer's request. Personal Data is incidental to the Company's Services. Based on Privacy by Design and Data Minimization principles, Company severely limits the instances of Personal Data collection and processing within the Services. Most use cases for porting Personal Data from Company are not applicable. However, Company will respond to all requests for data porting in order to address Customer needs.
Technical and organizational measures of sub-processors	The Company enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this DPA.

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

i.Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Company
Key Contact	*See* Exhibit B of this DPA	*See* Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

a) Annex 1A: List of Parties	b) As per Table 1 above
c) Annex 2B: Description of Transfer	*d) See Exhibit B of this DPA*
e) Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*f) See Exhibit C of this DPA*
g) Annex III: List of Sub processors (Modules 2 and 3 only):	*h) See Exhibit B of this DPA*

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

b) [SELECT OPTION] [*Note: This provision permits the selected party (if any) to terminate the UK Addendum if the ICO changes the approved UK Addendum which directly results in a substantial, disproportionate, and demonstrable increase in (a) its direct costs of performing its obligations under the UK Addendum or (b) its risk under the UK Addendum.]*

Ending this UK Addendum when the Approved UK Addendum changes	x Importer x Exporter ☐ Neither Party

i.

c) Entering into this UK Addendum:

1. Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

d) Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit D.
EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information
Appendix Information	shall be as set out in Table 3
Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 18 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.
ex-UK Transfer	shall have the same definition as set forth in the DPA .
UK	means the United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the DPA.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfills the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws will apply.

7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

e) **Hierarchy**

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

f) **Incorporation and Changes to the EU SCCs:**

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:

g) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

h) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and

i) the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.

13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.

15. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:

a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;

b) In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679",

c) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e) Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g) References to Regulation (EU) 2018/1725 are removed;

h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j) Clause 13(a) and Part C of Annex I are not used;

k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l) In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m) Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales";

n) Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales." A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts."; and

o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

j) **Amendments to the UK Addendum**

16. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved UK Addendum which:

a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

b) reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

c) its direct costs of performing its obligations under the UK Addendum; and/or

d) its risk under the UK Addendum,

1. and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

20. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.