MASTER SERVICES AGREEMENT

This Master Services Agreement ("Agreement") is entered into by and between Ellavox LLC, a Missouri limited liability company ("Ellavox"), whose address is 12747 Olive Blvd. Suite 300, St. Louis, MO 63141 and the Company ("Company" or "you") listed in an executed Statement of Work or Pilot Program Statement of Work (each, an "SOW") between Company and Ellavox. Ellavox and Company may each be referred to herein as a "Party" and collectively as the "Parties." The effective date of this Agreement is the earliest date of execution of any SOW entered into between the parties (the "Effective Date").

WHEREAS, Ellavox offers various Artificial Intelligence (AI) based products and services, and Company wishes to procure certain AI based products or services from Ellavox, subject to the terms of this Agreement and applicable Statement of Works (each a "SOW").

1. Defined Terms. The capitalized terms used in this Agreement shall, unless the context requires otherwise, have the meaning specified on Exhibit A, which is attached hereto and incorporated herein by reference. All Exhibits to this Agreement shall be incorporated herein by reference.

2. Structure of Agreement. This Agreement consists of (a) The general terms and conditions set forth herein; and (b) one or more SOWs (if any), each of which sets forth additional terms applicable to additional products or services procured by Company from Ellavox. In the event of a conflict between the terms of this Agreement and any SOW, the terms of the SOW shall govern with respect to the applicable product or Service, provided however, that any limitation of liability provisions in this Agreement shall govern or control over any limitation of liability provisions in an SOW.

3. Ellavox Obligations. Ellavox will comply in all material respects with all Laws applicable to Ellavox's provisioning of the Service(s) to its customers generally (i.e., without regard to the specific nature of the Company Data or Company's or any End-User's particular use of the Service.

4. Access to and Use of the Service

4.1 SOW. The specific details of the Services to be performed will be outlined in a SOW. Each SOW will be mutually agreed upon and executed by both parties. Each SOW shall be automatically subject to the terms of this Agreement.

4.2 Change Order. Unless otherwise specified in a SOW, Company may reasonably request in writing that revisions be made to the Service or deliverables, known as "Change Orders". Similarly, Ellavox may initiate a new SOW for Company's signature to formalize any changes

5. Certain Obligations of Company.

5.1 Compliance. Company shall comply with the Ellavox Platform & Services Terms set forth in Exhibit B.

5.2 Responsibility. Company shall be (a) be responsible for its End Users and Authorized Users compliance with this Agreement including without limitation Ellavox's Artificial Intelligence Acceptable Use Policy, which is attached hereto as Exhibit C and incorporated by reference, as it may be amended from time to time; (b) provide all required notices and obtain any licenses, permissions, and consents required, including (without limitation) under Applicable Data Protection Laws, from all End-Users, Authorized Users and others, for the collection of Company Data, including (without limitation) any Company Personal Data, under this Agreement and to enable Ellavox's access to, and Ellavox's use and other processing of such Company Data in connection with the Service; (c) be responsible for the accuracy,

completeness, appropriateness, and legality of Company Data; and (d) use the Service in accordance and compliance with all applicable laws and government regulations.

5.3 Usage Restrictions. Company shall not, and shall ensure that Authorized Users and End-Users do not, directly or indirectly: (a) make the Service or Output available to, or use the Service for the benefit of, anyone other than Company, its Authorized Users, and the End-Users; (b) upload, post, transmit, email, convey, or otherwise make available to Ellavox or the Service any content that (i) is unlawful or tortious or (ii) that infringes, misappropriates, or otherwise violates any intellectual property, privacy, publicity, or other proprietary rights of any person; (c) sublicense, resell, time- share, or similarly exploit the Service or Output; (d) upload, post, transmit, or otherwise make available any content or information designed to interrupt, interfere with, destroy or limit the functionality of any computer software or hardware or telecommunications equipment; (e) reverse engineer, modify, adapt, or hack the Service, or otherwise attempt to gain unauthorized access to the Service or its related systems or networks; or (f) access or use the Service to build a competitive product or service, or to assist a third party to do so.

5.4 Non-Ellavox Service(s). If Company elects to enable or use any Non-Ellavox Service(s) for use with the Service: (a) any use by Company, its Authorized Users, or End-Users of such products, services, or data is solely the responsibility of Company and is subject to the terms and conditions of such Non-Ellavox Service(s); (b) Ellavox does not endorse, is not responsible, liable for, or offer support for and makes no representations as to any aspect of such Non-Ellavox Service(s), including, without limitation, their content or the manner in which they handle, protect, manage or process data; (c) Ellavox cannot guarantee the continued availability of Non-Ellavox Service(s) and may temporarily or permanently cease providing, without entitling Company to refund, credit, or compensation, any particular Non-Ellavox Services and (d) Ellavox is not liable for any damage or loss caused or alleged to be caused by or in connection with Company's reliance on the privacy practices, data security processes or other policies of such Non-Ellavox Service(s). Company's use of any third-party software, services and other products is governed by the terms of any license or other agreement between Company and such third party.

5.5 Additional Usage Restrictions. Company agrees to notify Ellavox in writing that it requires Sensitive Data Managed Services (i) at least 30-days in advance of using the Service to transmit, store, collect, or otherwise process "Highly Sensitive Information", "Sensitive Data", "Special Categories of Personal Data" or similar terms defined in Applicable Data Protection Laws (together "Restricted Data"), and (ii) at least three (3) days prior to Ellavox and Company signing a SOW involving the use or access of Restricted Data. Depending on the Restricted Data, additional fees may be charged as set forth in the SOW. If Company does not provide the 30 day notice period herein or Company does not specifically contract with Ellavox to transmit, store, collect, or otherwise process Restricted Data, Company shall be solely responsible for any such use of the Service by Company, its' Authorized Users or its' End-Users, and Company shall indemnify, defend and hold harmless Ellavox from any liabilities, damages, costs and expenses for Ellavox's non-compliance with any Laws where such non-compliance is attributable to Company's use, receipt or provision of Restricted Data in connection with the Service.

5.6 Availability and Support. During the Term of each Service, Ellavox will provide support services in accordance with Ellavox's Support Policy which is set forth as Exhibit D, as it may be amended from time to time ("Support Policy"). Ellavox may update the Support Policy from time to time upon reasonable notice to the Company to reflect process improvements or changing practices, provided that such modifications do not materially decrease Ellavox's obligations as compared to those reflected in such terms as of the Effective Date. The terms of this Agreement will also apply to updates and upgrades of the Service subsequently provided by Ellavox. Ellavox may update the functionality, user interfaces, usability, and Documentation from time to time in its sole discretion as part of its ongoing mission to improve the Platform.

6. Fee; Invoicing; Taxes.

6.1 Fees; Invoicing and Payment. Company will pay all fees specified in the SOWs. Payment obligations are non-cancelable and, except as expressly set forth herein, fees paid are non-refundable. All fees will be invoiced by Ellavox in accordance with the terms set forth in the applicable SOW. Full payment for invoices issued must be received within thirty (30) days from Company's receipt of the invoice or in accordance with any different billing frequency stated in the applicable SOW. If any fees owed by Company (excluding amounts disputed in reasonable and good faith) have not been paid by the applicable due date, Ellavox reserves the right to apply a finance charge of 1.5% per month on any outstanding balance, or the maximum permitted by law, whichever is lower, and be reimbursed for all expenses of collection.

6.2 Taxes. The fees are exclusive of, and Company will be solely responsible for, all applicable taxes in connection with this Agreement, including but not limited to any sales, use, excise, transfer, value-added, goods and services, consumption, and other similar taxes or duties.

7. Proprietary Rights.

7.1 Ownership of Intellectual Property. Each Party retains all Intellectual Property Rights with respect to its intellectual property, including but not limited to any modifications, derivative works, upgrades, or updates thereto. No Intellectual Property rights are granted by either Party except as expressly set forth in this Agreement.

7.2 Ellavox Property. Subject to the limited rights expressly granted to Company hereunder, Ellavox reserves and retains, and as between Ellavox and Company, Ellavox exclusively owns, all rights, title, and interest in and to the Service, including, in each case, all modifications, derivative works, upgrades, and updates thereto, and all related Intellectual Property Rights therein. No rights are granted by Ellavox hereunder other than as expressly set forth herein. If Company, any Authorized User, or any End-User provides Ellavox any feedback or suggestions regarding the Service, then Company grants or, as applicable, shall cause such End-User to grant Ellavox an unlimited, irrevocable, perpetual, sublicensable, royalty-free license to use any such feedback or suggestions for any purpose without any obligation or compensation to such person or entity. Unless otherwise expressly set forth in a SOW, Ellavox retains exclusive ownership of all work product created by Ellavox in connection with its performance of the Platform and the Services.

7.3 Company Data. As between Company and Ellavox, Company owns all rights, title, and interest in and to the Company Data. Company hereby grants, and shall cause all End-Users to grant, to Ellavox a worldwide, irrevocable, non-exclusive, fully paid, royalty-free, transferable, and perpetual right and license, with rights to sublicense (i) to access, use, copy, create derivative works from, distribute, perform, and display Company Data for purposes of providing the Service and Non-Ellavox Services and (ii) the right to create and/or derive from Company Data de-identified, anonymized and/or aggregated data ("Anonymized Data") that does not identify Company or any End-User and, both during and after the Term. Anonymized Data shall be considered Ellavox's data.

8. Confidentiality.

8.1 "Confidential Information". The term "Confidential Information" means all confidential or proprietary information disclosed by a Party ("Disclosing Party") to the other Party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including all copies thereof. Confidential Information will not include any information that: (a) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (b) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (c) is received from a third party without breach of any obligation owed to the Disclosing Party; or (d) was independently developed by the Receiving Party without any use of the Disclosing Party's Confidential Information.

8.2 Protection of Confidential Information. The Receiving Party will: (a) use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care); (b) not use any Confidential Information of the Disclosing Party for any purpose not permitted by this Agreement; and (c) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of the Receiving Party's employees, contractors, and agents who need such access for purposes consistent with this Agreement and who are subject to confidentiality obligations at least as restrictive as those herein. The Receiving Party will provide prompt written notice to the Disclosing Party of any unauthorized use or disclosure of the Disclosing Party's Confidential Information. Upon request of the Disclosing Party during the Term, the Receiving Party will promptly return, or at the Disclosing Party's option destroy, any or all Confidential Information of the Disclosing Party in the Receiving Party's possession or under its control.

8.3 Compelled Disclosure. The Receiving Party may access or disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled access or disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's expense, if the Disclosing Party wishes to contest the access or disclosure.

9. Representations and Disclaimers.

9.1 Mutual Representations. Each Party represents and warrants that: (a) it is duly organized, validly existing, and in good standing under its jurisdiction of organization and has the right to enter into this Agreement; (b) the execution, delivery, and performance of this Agreement are within the corporate or limited liability company powers of such Party and have been duly authorized by all necessary corporate or limited liability company action on the part of such Party, and constitute a valid and binding agreement of such Party, and (c) there is no outstanding claim, litigation, proceeding, arbitration, investigation or material controversy to which such Party is a party that would reasonably be expected to have a material adverse effect on such Party's ability to enter into this Agreement or perform any of its material obligations hereunder.

9.2 Representations of Company. Company represents and warrants that: (a) it has obtained and will maintain all rights, consents, and permissions necessary for Company and the Authorized Users and End-Users to make available to Ellavox, and for Ellavox to use as contemplated herein, all Company Data; and (b) the Company Data will not infringe, misappropriate, or otherwise violate any intellectual property, privacy, publicity, or other proprietary rights of any person or entity, or violate any applicable laws or government regulations.

9.3 Disclaimer. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES PROVIDED IN THIS AGREEMENT, THE ELLAVOX SERVICES (INCLUDING BUT NOT LIMITED TO THE PLATFORM AND ANY AGENT SERVICES) AND ALL RELATED COMPONENTS AND INFORMATION ARE PROVIDED ON AN "AS IS, AS AVAILABLE" BASIS WITHOUT ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, AND ELLAVOX EXPRESSLY DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS WARRANTIES, WHETHER EXPRESS, IMPLIED ORAL OR WRITTEN, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ELLAVOX DOES NOT REPRESENT WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE NOR THAT THE SERVICE WILL MEET COMPANY'S OR ANY END-USER'S REQUIREMENTS. ELLAVOX FURTHER DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO ANY THIRD PARTY PRODUCTS.

10. Indemnification.

10.1 Ellavox Indemnification. Ellavox will defend Company from and against any lawsuit or proceeding brought by a third party to the extent alleging that Company's use of the Service as permitted hereunder infringes or

misappropriates such third party's intellectual property rights, and Ellavox will indemnify Company for any damages and any reasonable attorneys' fees finally awarded against it arising from such lawsuit or proceeding; provided, however, that Ellavox will have no liability under this Section to the extent any such lawsuit or proceeding arises from: (a) Company Data, any Non-Ellavox Services, Third Party LLM Providers, or any other third-party provided products, services, or data; (b) Company's, any of its Authorized Users', or any End-Users' negligence, misconduct, or breach of this Agreement; (c) any modification or combination of the Service that is not performed by Ellavox; (d) any use of the Service that is contrary to any written instructions provided by Ellavox, or (e) claims arising out of any unauthorized use of the Service.

10.2 Company Indemnification. Company will defend Ellavox from and against any lawsuit or proceeding brought by a third party to the extent alleging that: (a) any Company Data infringes, misappropriates, or otherwise violates the rights, including privacy and publicity rights, of any other party; (b) Company has breached any of its obligations under Section 5; or (c) Company's or any Authorized User's or End-User's particular use of the Service or use or provision of any Company Data violates any applicable Laws. Company will indemnify Ellavox and its Affiliates for any damages and any reasonable attorneys' fees finally awarded against them arising from such lawsuit or proceeding; provided, however, that Company will have no liability under this Section to the extent any such lawsuit or proceeding arises from Ellavox's gross negligence or breach of this Agreement.

10.3 Procedures. The indemnified Party will provide the indemnifying Party with: (a) prompt written notice of any matter that is subject to indemnification hereunder; and (b) the right to assume the exclusive defense and control of any such matter (provided that the indemnifying Party may not settle any claim unless it unconditionally releases the indemnified Party of all liability and receives indemnified Party written approval (which shall not be unreasonably withheld) of any conditions imposed by the settlement, if applicable. The indemnified Party will reasonably cooperate with any reasonable requests assisting the indemnifying Party's defense of such matter.

11. Limitation of Liability.

11.1 Exclusion of Certain Damages. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT OR ANY SOW TO THE CONTRARY, TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, OR PUNITIVE DAMAGES, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.2 Liability Cap. EXCEPT FOR COMPANY'S LIABILITY FOR ITS PAYMENT OBLIGATIONS UNDER SECTION 6 OR A PARTY'S LIABILITY FOR ITS INDEMNIFICATION OBLIGATIONS UNDER SECTION 10, OR ITS WILLFUL MISCONDUCT, IN NO EVENT WILL A PARTY'S MAXIMUM'S AGGREGATE LIABILITY ARISING FROM OR RELATING TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID OR PAYABLE BY COMPANY TO ELLAVOX HEREUNDER IN THE TWELVE (12) MONTHS PRECEDING THE DATE ON WHICH THE FIRST CLAIM GIVING RISE TO LIABILITY AROSE.

11.3 Scope. For the avoidance of doubt, the exclusions and limitations set forth in Section 11.1 and Section 11.2 will apply with respect to all legal theories of liability, whether in contract, tort, or otherwise. The Parties agree that the exclusions and limitations set forth in Section 11.1 and Section 11.2 allocate the risks between the Parties under this Agreement, and that they have relied on these exclusions and limitations in determining whether to enter into this Agreement.

12. Term, Termination and Suspension.

12.1 Term. The term of this Agreement commences on the Effective Date and, unless earlier terminated in accordance with the terms of this Agreement, will continue until the last SOW expires or is earlier terminated in

accordance with this Agreement (the "Term").

12.2 Suspension. Ellavox reserves the right to immediately suspend Company's or any Authorized Users' access to the Service, in whole or in part, if: (a) Company, an Authorized User or an End-User violates the terms of this Agreement or any applicable Laws; (b) Company's or any Authorized Users' systems or accounts have been compromised or unlawfully accessed; (c) Ellavox reasonably believes that suspension is necessary to protect the security of the Services or the infrastructure of Ellavox or its Affiliates; (d) suspension is required by applicable Law; or (e) if any fees owed by Company (excluding amounts disputed in reasonable and good faith) are overdue and Company fails to cure such breach within seven (7) days after receiving written notice of such breach. In addition to the aforementioned rights of suspension, Ellavox's right to suspend shall not release Company from its obligation to continue to pay any fees or charges due during the period of suspension. Company acknowledges that suspension of the Services shall not constitute a waiver or release of Company's payment obligations under this Agreement.

12.3 Termination for Force Majeure. Ellavox may, upon 10 days proper written notice, terminate this Agreement upon the occurrence of a Force Majeure Event (as defined in Section 13.2) whereby Ellavox is not able to perform all or a material portion of its obligations hereunder due to such Force Majeure Event for a period of 30 consecutive days.

12.4 Termination for Cause. Either Party may terminate this Agreement, effective 30 days' after written notice, if the other Party materially breaches this Agreement and such breach is not cured within such 30-day period. Upon any such termination for cause by Company, Ellavox will promptly refund Company any prepaid fees covering the period remaining in the Term after the effective date of such termination. Upon any such termination for cause by Ellavox, Company will promptly pay Ellavox any unpaid fees covering the period remaining in the Term after the effective date of such termination.

12.5 Effects of Termination. In no event will any termination of this Agreement relieve Company of its obligation to pay any fees accrued or payable to Ellavox for the period of time prior to the effective date of such termination. Upon any termination of this Agreement, Company and all Authorized Users and End-Users must immediately cease all use of the Services. Additionally, the Receiving Party must promptly return, or at the Disclosing Party's option, destroy, any or all Confidential Information of the Disclosing Party in the Receiving Party's possession or under its control.

12.6 Survival. Each provision of this Agreement that would by its nature or terms survive any termination of this Agreement shall survive the expiration or earlier termination of this Agreement, regardless of the cause. Such provisions include, without limitation, Sections 5, 6, 7, 8, 9, 10, 11, 12 and 13. Any action of any kind arising out of or in any way connected with this Agreement, other than collection of outstanding payment obligations by Ellavox, shall be barred unless such action is commenced within two (2) years of the date upon which the cause of action accrues.

13. Miscellaneous.

13.1 Attribution. Company agrees that Ellavox may use Company's name and logo to indicate that Company is a customer of Ellavox for the Service on Ellavox's website, marketing materials, and in communications with existing or prospective Ellavox customers. Any such attribution will be consistent with Company's style guidelines or requirements as communicated in writing to Ellavox by Company. Company has the right to revoke this consent to be used as a reference customer upon written notice to Ellavox if Ellavox violates the foregoing, and in such case, Ellavox will use reasonable efforts to promptly remove all use of Company's name and logo on websites, and to cease future use of Company's name and logo on marketing materials.

13.2 Force Majeure. Except for payment obligations, neither Party will be liable hereunder by reason of any failure or delay in the performance of its obligations due to events beyond the reasonable control of such Party, which

may include natural disasters, fires, epidemics, attacks (nuclear, cyber, chemical or biological), pandemics, riots, war, terrorism, denial of service attacks, internet or power outages, labor shortages, travel restrictions, delay of vendors, and judicial or government action (each a "Force Majeure Event"). The party experiencing a Force Majeure Event, shall use commercially reasonable efforts to provide notice of such to the other party.

13.3 Assignment. Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other Party. Notwithstanding the foregoing, either Party may assign or transfer this Agreement in its entirety, without the consent of the other Party, in connection with a merger or sale of all or substantially all of its assets, provided however, that if Company is the assigning or transferring party, Ellavox's consent shall be required unless Company is current on payment of all fees owed to Ellavox and Company can provide evidence to Ellavox that Company's assignee's or transferee's financial net worth is at least equal to or greater than Company's financial net worth. Any purported assignment in violation of this Section will be null and void. This Agreement will bind and inure to the benefit of the Parties, their respective successors, and permitted assigns.

13.4 Law; Venue. This Agreement, and any disputes arising out of or related hereto, will be governed exclusively by the internal laws of the State of Delaware, without regard to its conflicts of laws rules or the United Nations Convention on the International Sale of Goods

13.5 Dispute; Arbitration. The parties will attempt in good faith to resolve any disputes under this Agreement. Each party will designate an officer with the responsibility and the authority to resolve the dispute. These officers will meet within fifteen (15) days after the request to identify the scope of the dispute and the information needed to discuss and attempt to resolve such dispute. These officers will then gather relevant information regarding the dispute and will meet to discuss the issues and to negotiate in good faith to resolve that issue. If the Parties are unable to resolve the dispute within thirty (30) days after the specific meeting of the designated officers as specified above (or such longer time as the Parties agree), then the dispute will be resolved by binding arbitration under the terms of this Section 13.5, except as set forth herein. Such arbitration will be conducted in St. Louis County, Missouri, in accordance with the rules then in effect of the American Arbitration Association ("AAA") by an arbitrator who (a) has substantial data processing and/or information technology experience and/or AI experience and (b) is appointed in accordance with such rules (or is mutually agreed upon by the parties). The arbitration, while subject to the rules of the AAA, does not have to be administered by the AAA (unless both parties mutually agree to it). The award rendered by the arbitrator will be final and binding, and judgment may be entered upon it in any court having jurisdiction thereof. The failure of either party to exercise any rights granted hereunder shall not operate as a waiver of any of those rights. This Agreement concerns transactions involving commerce among the several states. The arbitrators will not be empowered to award punitive damages. If this Agreement is found not to be subject to arbitration, the parties knowingly and willingly waive any right they have under applicable Law to a trial by jury in any dispute arising out of or in any way related to this Agreement or the issues raised by that dispute.

Notwithstanding anything contained in this Agreement to the contrary including the preceding provisions of this Section 13.5, (i) Ellavox may bring any action against Company with respect to the collection of outstanding payment obligations (the "Section 13.5 Matters") in the state courts sitting in St. Louis County, Missouri or the United States District Court for the Eastern District of Missouri, without any requirement or obligation to utilize the provisions referenced in the first paragraph of Section 13.5 above and (ii) the Parties consent to exclusive jurisdiction and venue of such courts (and of the appropriate appellate courts) with respect to Section 13.5 Matters. Each Party irrevocably waives any and all rights to a trial by jury in any legal proceeding arising out of or related to the Section 13.5 Matters.

13.6 Notices. All notices under this Agreement will be in writing addressed to the Parties at the addresses set forth on the first page of this Agreement and will be deemed to have been duly given: (a) upon receipt if personally delivered

or sent by certified or registered mail with return receipt requested; and (b) the first business day after sending by email or by next day delivery by a recognized overnight delivery service. Each Party may change its written address for notice by written notice to the other Party.

13.7 Export Control and Economic Sanctions. Each Party: (a) agrees to comply with all export control and economic sanctions and relevant import laws of the United States and other applicable jurisdictions, and (b) represents and warrants that it is not listed on any U.S. or other government list of prohibited or restricted parties or located in (or a national of) a country that is subject to a U.S. government export control embargo or economic sanctions. Without limiting the foregoing, (a) Company will not (and will not permit any of its End-Users to) access and use the Service in violation of any U.S. export control or economic sanction, prohibition or restriction, and (b) Company will not submit to the Service any information that is controlled under the U.S. International Traffic in Arms Regulations or applicable international import and export laws and regulations.

13.8 Relationship of the Parties; Third Party Beneficiaries. The Parties are independent contractors and this Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties. Nothing in this Agreement shall confer upon any person or entity other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

13.9 Waiver. No failure or delay by either Party in exercising any right under this Agreement will constitute a waiver of that right.

13.10 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, such provision will be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement will remain in full force and effect.

13.11 Entire Agreement. This Agreement, including all SOWs and Exhibits, constitutes the entire agreement between the Parties and supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning the subject matter herein. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by each of the Parties. To the extent of any conflict or inconsistency between the terms of this Agreement and any SOW, the terms of this Agreement will prevail, unless the SOW expressly modifies a particular provision of this Agreement. Notwithstanding any language to the contrary therein, no terms or conditions stated in any Company purchase order or other Ellavox order documentation (excluding SOWs) will be incorporated into or form any part of this Agreement, and all such terms or conditions will be null and void. As used herein, the words "include" and "including" shall be deemed to be followed by the words "without limitation."

13.12 Authority. If you are entering into this Agreement on behalf of a company, organization, or other entity, you represent that you have the authority to bind such company, organization, or other entity.

In the event Company and Ellavox execute a Statement of Work that references this Agreement, then the terms of this Agreement shall become part of the SOW. Should there be any conflict between the terms of the SOW and this Agreement, the terms of the SOW shall take precedence.

EXHIBIT A

DEFINITIONS

Capitalized terms in this Agreement shall have the meanings set forth in this Exhibit A unless defined elsewhere.

"Applicable Data Protection Laws" means the privacy, data protection and data security laws and regulations of any jurisdiction directly applicable to Ellavox's Processing of Company Personal Data under the Agreement (including, as and to the extent applicable, the CCPA and GDPR).

"Authorized User" means an employee, representative or contractor of Company who is authorized by Company to access and use the Service on behalf of and solely for the benefit of Company.

"CCPA" means California Consumer Privacy Act, as it may be amended from time to time.

"Company Personal Data" means any Personal Data contained within Company Data and Processed by Ellavox in order to perform the Service.

"Company Data" means all data and content submitted, transmitted, or uploaded into the Service by Company, Authorized Users, or End-Users.

"Deliverable" means any tangible or intangible output, result or product provided to the Company as a result of Ellavox's performance of Professional Services, as specified in the applicable SOW.

"Documentation" means the documentation, specifications, and policies, as may be updated from time to time, that describe the functionality, features, operation, or use of the Service and that are made available by Ellavox to Company.

"End-User" means an individual end-user who is authorized by Company to access and use the Services or to whom the Company makes the Services available.

"GDPR" means The General Data Protection Regulation (EU) 2016/679, as it may be amended from time to time.

"Intellectual Property Rights" means all past, present, and future rights of the following types, which may exist or be created under the laws of any jurisdiction in the world: (a) rights associated with works of authorship, including exclusive exploitation rights, copyrights, moral rights, and mask works; (b) trademark and trade name rights and similar rights and their associated goodwill; (c) trade secret rights; (d) patents and industrial property rights; (e) other proprietary rights in intellectual property of every kind and nature; and (f) rights in or relating to registrations, renewals, extensions, combinations, divisions, and reissues of, and applications for, any of the rights referred to in subsections (a) through (e) of this sentence.

"LLM" means an AI large language model.

"Non-Ellavox Service(s)" means any third-party provided applications, networks, software, products, or services which Company may connect to or incorporates into, or otherwise leverages in connection with the Service.

"Output" means all answers and results generated by one or more Third-Party LLM Providers based on Inputs and made available via the Platform.

“Managed Services” means any ongoing support services provided by Ellavox to support Company and Company’s use of the Services and Platform, such as data backups, data security services, security compliance monitoring, and performance monitoring among others as identified in an SOW between Ellavox and Company.

“Personnel” means a Party’s officers, directors, employees, managers and authorized agents, and for Ellavox, any approved subcontractors contributing to this Agreement’s obligations. For purposes of the foregoing, a Party’s Personnel shall not be considered Personnel of the other Party.

“Personal Data” means “personal data,” “personal information,” “personally identifiable information” or similar term as defined in Applicable Data Protection Laws.

“Platform” means Ellavox’s software-as-a-service platform provided to Company as part of the Service(s), which is distinct from the Support Services and any Non-Ellavox Services.

“Process” and inflections thereof means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Professional Services” means any professional services related to Company’s use of the Service, such as configuration, implementation, or training services, provided by Ellavox to Company as expressly identified in a SOW.

“Sensitive Data Managed Services” means the Managed Services provided by Ellavox for the Platform and Services utilized by Company in order to safeguard the transmission, storage, collection, or otherwise processing of “Highly Sensitive Information”, “Sensitive Data”, “Special Categories of Personal Data” or similar terms defined in Applicable Data Protection Laws (together “Restricted Data”).

“Service(s)” means, collectively, as identified in a SOW, Ellavox’s provision of the Platform and the associated capabilities of the Platform, and any Managed Services or Sensitive Data Managed Services to support the Platform and Company. Any references to the “Service(s)” in this Agreement includes the Documentation but excludes Non-Ellavox Services.

“SOW” means each statement of work entered into and executed by each of the Parties that references this Master Services Agreement. Each SOW forms a part of, and is incorporated into, this Master Services Agreement.

“Subscription Term” means the period during which Company has agreed to subscribe to the Service as specified in an applicable SOW.

“Third-Party LLM Provider(s)” means any entity providing a LLM retained or used by Ellavox to provide certain AI features, including but not limited to chatbot functionality, which leverages artificial intelligence technology provided by third party companies.

EXHIBIT B:

ELLAVOX PLATFORM & SERVICES TERMS

The terms contained in this Exhibit B are specifically applicable to the Platform and the associated Services provided by Ellavox under this Agreement. These terms outline the specific functionalities, warranties, obligations, and any limitations associated with the use of Ellavox's Platform & Services. The following provisions are intended to supplement the general terms of the Agreement and should be read in conjunction with the main body of the Agreement. Capitalized terms used in this Exhibit may be defined in Exhibit A of this Agreement.

1. Ellavox Responsibilities

1.1 Provision of the Platform and Services. Subject to the terms and conditions of this Agreement and during the Term, Ellavox will: (a) make the Platform and Services available to Company for use by Authorized Users solely for the business operations of Company and its End-Users (which may include customers, employees, vendors, or anyone or any system communicating with Company) via Company's communication channels including its website, chat, text/SMS, email, phones, and mobile applications as agreed to in a SOW; (b) provide Company with Managed Services and standard support services and Documentation to assist Company in its use of the Services; (c) comply in all material respects with all Laws applicable to the provisioning of the Services to its customers generally; and (d) provide updates and upgrades to the Platform and Services, including functionality, user interfaces, usability, and Documentation, in its sole discretion as part of its ongoing mission to improve the Platform and Services.

1.2 Platform Accounts. Company must identify a primary Authorized User who will be responsible for Company's account within the Platform. Ellavox shall be responsible for creating Authorized User accounts for the Platform. Company is responsible for (i) maintaining the confidentiality of its logins, passwords, and accounts and for all activities that occur under Authorized User accounts, (ii) securing the systems and devices Company and Authorized Users use to access the Platform, and (iii) backing up Company Data provided to Ellavox and utilized by the Platform and Services.

1.3 Beta or Pilot Services. From time to time, Ellavox may invite Company to try or otherwise make Beta or Pilot Services available to Company at no charge. Company may accept or decline any such Beta or Pilot Services in Company's sole discretion. Beta or Pilot Services are: for evaluation purposes only; not for production use; not supported; and may be subject to additional terms. Beta or Pilot Services are not considered "Services" under this Agreement and are to be used for Company's internal testing and evaluation purposes only and are not subject to the same security measures specified in the Documentation. If Company, any Authorized User, or any End-User provides Ellavox any feedback or suggestions regarding the Beta Services, then Company grants or, as applicable, shall cause such End-User to grant Ellavox an unlimited, irrevocable, perpetual, sublicensable, royalty-free license to use any such feedback or suggestions for any purpose without any obligation or compensation to such person or entity. Ellavox may discontinue Beta or Pilot Services at any time in Ellavox's sole discretion and may or may not make them generally available. Ellavox will have no liability arising out of or in connection with any Beta or Pilot Service and disclaims any warranty, indemnity, support, service level agreement or other obligations with respect to Beta or Pilot Services. Company uses Beta or Pilot Services "As-Is", and at its own risk.

2. Access to and Use of the Service(s)

2.1 Company Responsibilities: Company will use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and promptly notify Ellavox of any such unauthorized access or use;

2.2 AI Features - Third-Party LLM Providers. The Platform offers certain features and functionality that utilize artificial intelligence ("AI Features"), powered by large language models provided by Third Party LLM Provider(s). Upon Company's instructions, Ellavox will upload all materials, policies, guidelines, manuals and other documentation that is created, owned and provided by Company (collectively "Company Documentation") into the Platform for the purpose of utilizing the AI Features. The Company acknowledges that the AI Features, which employ artificial intelligence technology based on the Company Documentation, will use any prompts, comments, questions, and other forms of input provided by the Company or End-Users "Input" to generate the Output in accordance with the terms of this Agreement. The Company further accepts that the AI Features may produce Output that could be inaccurate, misleading, or inappropriate. Company is solely responsible for the accuracy and completeness of the Company Documentation provided to Ellavox. As AI Features operate based on the Input, the resulting Output may be inaccurate or inappropriate if the Input is flawed. Company agrees, and shall cause End-Users to agree in the End-User Terms, that it is solely responsible for its use of AI Features. Accordingly, all Outputs are provided "as is" and with "all faults", and Ellavox makes no representations or warranties, or provides any indemnities, of any kind or nature with respect to the AI Features, Inputs, or Outputs, including any warranties of accuracy, completeness, truthfulness or fitness for a particular purpose. Inputs and Outputs are deemed Company Data under this Agreement and subject to the rights, restrictions and obligations applicable thereto. Company acknowledges that other users of the Service or AI Features may provide similar or identical Input and as such, may receive Output ("Third Party Results") that is similar or identical to that of Company, and Company acknowledges it has no right, title or interest in or to any such Third Party Results. Company agrees that Ellavox shall have no responsibility or liability arising from the provision of inaccurate or inappropriate Output or any decisions made in reliance on such Output. All such decisions are made at Company's own risk.

3. Confidentiality

3.1 Confidential Information Specific to Ellavox Services. Within the context of Ellavox services, "Confidential Information" also includes the Services (including its software and content) and the work product resulting from Ellavox's performance of Professional Services or Managed Services, excluding the Deliverables. For Company, Confidential Information includes the Company Data and Company Data included in the Output.

4. Warranties

4.1 Ellavox Warranties. Ellavox warrants that: (a) the Service will perform materially in accordance with the applicable Documentation; (b) Ellavox will not materially decrease the functionality of the Platform; and (c) Ellavox will perform the Managed Services and the Professional Services in a professional manner. If Ellavox breaches any of the foregoing warranties in this Section, Company's exclusive remedy and Ellavox's entire liability will be the correction of the breach, or if Ellavox cannot substantially correct the breach within a commercially reasonable amount of time, Company may terminate this Agreement and Ellavox will refund to Company any prepaid fees covering the period remaining in the Term after the effective date of such termination.

5. Termination

5.1 Effects of Termination Specific to the Platform Upon termination of the Platform services, the Company and all Authorized Users and End-Users must immediately stop using the Platform and any related Output. Upon request of the Disclosing Party during the Term, the Receiving Party will promptly return, or at the Disclosing Party's option destroy, any or all Company Data of the Disclosing Party in the Receiving Party's possession or under its control.

EXHIBIT C

SUPPORT POLICY

This Support Policy outlines the support services provided by Ellavox ("we" or "our") to Company ("you" or "your"). Our goal is to provide you with exceptional service and support to ensure the highest level of customer satisfaction.

Support Services

We offer support services to assist with any technical issues or questions related to our Services. Our support team is available during the following hours:

- Business Hours: Monday to Friday, 9 AM to 6 PM EST
- After-Hours Support: N/A - during Business Hours, our support team will prioritize responding to after-hours requests based on the severity of the request as outlined in the "Response Times" section below.
- Support requests can be submitted through the following channels:

Email: support@ellavox.ai

Response Times

Our support team aims to respond to all inquiries within the following timeframes:

- Critical Issues: Within 2 Hours during Business Hours
- High Priority Issues: Within 4 Hours during Business Hours
- Normal Priority Issues: Within 1 Business Day during Business Hours
- Low Priority Issues: Within 2 Business Day during Business Hours

Support Tiers

We offer the following tiers of support:

- Tier 1: Basic troubleshooting and issue resolution.
- Tier 2: In-depth technical support and issue escalation.
- Tier 3: Advanced support involving our engineering team for complex issues.

Exclusions

Our support services do not cover the following:

- Issues resulting from Company's modifications to the Service offering not in accordance with our Documentation.
- Support for third-party applications or services not provided by us.
- Training on the use of the SaaS offerings (available separately).
- Company's equipment, software network connections or other infrastructure.
- General Internal problems, force majeure events or other factors outside of Ellavox's reasonable control.

Updates and Maintenance

We regularly update and maintain our Service to improve functionality and security. You will be notified of scheduled maintenance and updates in advance.

Contact Us

support@ellavox.ai

EXHIBIT D

ARTIFICIAL INTELLIGENCE ACCEPTABLE USE POLICY

1. Scope

A. This Artificial Intelligence Acceptable Use Policy ("Policy") applies to customers' use of all services offered by Ellavox LLC or its affiliates ("Ellavox"), or third-party products, applications or functionality that interoperate with services offered by Ellavox, that incorporate artificial intelligence (collectively, "Covered AI Services"). Within the Covered AI Services, those that use Generative AI will be referred to as the "Covered Generative AI Services."

2. Last Updated

A. September 11, 2025

3. Changes to Policy

A. Ellavox may change this Policy by providing an updated version of the Policy to the customer ("Company") or posting it on the Ellavox website.

4. Violations

A. Company's violation of this Policy will be considered a material breach of the Master Services Agreement ("MSA") and/or other agreement governing the customer's use of the services.

5. Disallowed Usage:

A. A Company may not use a Covered AI Service, nor allow its users (i.e. Authorized Users or End Users, as each is defined in the MSA) or any third party to use a Covered AI Service, for the following:

I. Automated Decision-Making Processes with Legal Effects
a. As part of an automated decision-making process with legal or similarly significant effects, unless:
i. such Company ensures that the final decision is made by a human being and takes other factors beyond the Services' recommendation into account; and
ii. such Company is transparent about the role of the Covered AI Service and the logic involved in the decision-making process, including providing subjects of the decision with the right to receive an explanation of the role of the Covered AI Service in the decision-making and the main reasons for the decision.
b. As part of an automated decision-making process for payday lending even when the final decision is made by a human being.

II. Individualized Advice from Licensed Professionals
a. Generating individualized advice that in the ordinary course of business would be provided by a licensed professional. This includes, for example, financial and legal advice.
b. Generating or providing individualized medical advice, treatment, or diagnosis to a consumer or end user.
c. For clarity, this section does not limit a Company from using Covered AI Services for other purposes, such as customer support in regulated industries, or to assist a licensed professional where Covered AI Services were not

leveraged in the generation of individual advice. When a Company uses such services to assist in providing individualized advice (e.g., summarization), there must be a qualified person reviewing the output.

III. Explicitly Predicting Or Categorizing Based On Protected Characteristics

a. Explicitly predicting, or categorizing based on an individual's protected characteristic, including, but not limited to, racial or ethnic origin, and past, current, or future political opinions, religious or philosophical beliefs, trade union membership, age, gender, sex life, sexual orientation, disability, health status, medical condition, financial status, criminal convictions, or likelihood to engage in criminal acts.

i. The previous sentence does not limit or prohibit use cases or tools designed specifically to identify security breaches, unauthorized access, fraud, and other security vulnerabilities, or to identify and reduce bias in the Ellavox Services.

ii. Additionally, Company may not submit images, videos or audio recordings of individuals for the purposes of creating, analyzing, or categorizing based on biometric identifiers, such as face prints or fingerprints or scans of eyes, hands, voiceprints, or facial geometry.

IV. Social Scoring and Crime Prediction

a. Evaluating, classifying, scoring or rating individuals or groups based on their social behavior or personality characteristics where such scoring leads to:

i. Detrimental or unfavorable treatment unrelated to the original context of the collected data; or

ii. Unjustified or disproportionate treatment relative to the assessed behavior.

b. Assessing or predicting the risk of an individual committing a criminal offense, based solely on profiling or assessing their personality traits and characteristics.

V. Emotion and Facial Recognition

a. Detecting, inferring, or assessing individuals' emotions in the workplace or in educational institutions, except for medical or safety reasons.

b. Creating or expanding facial recognition databases, e.g., through scraping facial images from the Internet or from CCTV footage.

c. Using real-time biometric recognition in public spaces for law enforcement purposes, unless an exception is expressly permitted by applicable law (e.g., to prevent a serious threat or find a missing person).

VI. Deceptive Activity

a. Engaging in plagiarism or academic dishonesty.

b. Deploying subliminal, purposefully manipulative or deceptive techniques that impair an individual's ability to make an informed decision.

c. Exploiting vulnerabilities of individuals, e.g., due to their age, disability or specific social or economic situation.

VII. Child Exploitation and Abuse

a. Creating, sending, uploading, displaying, storing, processing, or transmitting material that may be harmful to minors including, but not limited to, for any purposes related to child exploitation or abuse, such as real or artificial Child Sexual Abuse Material (CSAM).

B. Company may not use a Covered AI Service, nor allow its users or any third party to use any Covered AI Services, for the following:

I. Weapons Development

a. Developing, advertising, marketing, distributing, or selling weapons, weapon accessories, or explosives, as enumerated by the United States Munitions List.

II. Political Campaigns

a. Targeting, creating, or distributing political campaign materials for external public or semi-public audiences. Political campaign material refers to material:

i. That may influence a political process, such as an election, passage of legislation, regulation or ballot measure, judicial ruling, and content for campaigning purposes; or

ii. Soliciting financial support for (i)

III. Adult Content.

a. Creating, sending, uploading, displaying, storing, processing or transmitting sexually explicit material;

b. Creating, sending, uploading, displaying, storing, processing or transmitting sexual chatbots or engaging in erotic chat.

6. Use Notice and Disclosures

A. USE NOTICE: AI technology, including Generative AI, will continue to be used in new and innovative ways. Company is responsible for determining if its use of these technologies is appropriate for its business.

B. If required by law, Company shall: (i) disclose to end users when they are interacting directly with automated AI systems, including but not limited to Ellavox AI bots or voice agents or similar features unless there is a human in the loop; and (ii) provide a means for end users to interact with a human instead of an automated system.

C. If required by law, Company shall disclose to individuals when exposing them, for the limited purpose permitted in this Policy, to an emotion recognition system or a biometric categorization system.

D. Company may not deceive end users or consumers by misrepresenting content generated through automated means as human generated or original content.

EXHIBIT E

EU and UK Data Processing Addendum

This EU and UK Data Processing Addendum ("DPA") supplements the Ellavox LLC Master Services Agreement (the "Agreement") entered into by and between the customer signing this DPA ("Customer") and Ellavox LLC, Inc. ("Company") By executing the DPA in accordance with Section 11 herein, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if any. This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Agreement.

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: (i) the California Consumer Privacy Act ("CCPA"), (ii) 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"), (iii) the Swiss Federal Act on Data Protection, ; (iv) the UK Data Protection Act 2018; and (v) 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 "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), as modified by Section 6.2 of this DPA.

1.9 "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.

1.10 "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.

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

1.12 "Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

1.13"UK SCCs" means the EU SCCs, as amended by the UK Addendum.

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. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith.

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.

1.1 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.

2.3 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 (as applicable) shall be provided by Company to Customer only upon Customer's request.

2.4 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 information from Customer in order to provide the Services pursuant to the Agreement, which constitutes

a business purpose. Company shall not sell any such personal information. Company shall not retain, use or disclose any personal information provided by Customer pursuant to the Agreement 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 "personal information," "service provider," "sale," and "sell" 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 https://www.ellavox.ai/privacy/subprocessors. 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 Company's technical and organizational security measures.

6. Transfers of Personal Data

6.1 The parties agree that 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 the United States, and that the transfer of Customer's Personal Data to the United States 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:

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 the GDPR to conduct a 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 GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.3 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records for a period of three (3) years after the termination of the Agreement. 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.ellavox.ai/privacy policy.

10. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) the Company's privacy policy. 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@ellavox.ai. Upon receipt of the validly completed Addendum by Company at this email address, this DPA will become legally binding.

Customer	**Ellavox LLC**
Signature:	Signature:

Customer Legal Name:	
Print Name:	Print Name:
Title:	Title:
Date:	Date:

Data Processing Addendum 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 subprocessors 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 Personnel: Employees, contractors, administrators, and authorized users of the Customer using the Ellavox SaaS or Elacity platform.
● Customer's End-Users / Clients ("Customers' Customers"): Individuals interacting with or communicated with by Ellavox AI Voice Agents (e.g., apartment tenants/applicants, logistics contacts, drivers, customer service callers).

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:
● Contact & Identification Data: Name, phone number, email address, physical mailing address. ● Voice & Interaction Data: Call recordings, audio streams, voice transcripts, call metadata (timestamp, call duration, caller ID).
● Operational & Transactional Data: Tenant/apartment inquiry details, maintenance request records, leasing details, dispatch/logistics notes, account/collections status notes.
● Technical & Usage Data: IP addresses, login credentials, user access logs, browser/device metadata, activity logs within the platform.

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**.**

Data Processing Addendum 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: Ellavox LLC.

Trading Name (if different): Ellavox AI

Address and contact information: 12747 Olive Blvd Suite 300, St Louis MO 63141; privacy@ellavox.ai Official Registration Number (if any) (company number or similar identifier): N/A

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 at: https://www.ellavox.ai/privacy/subprocessors.

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.

Data Processing Addendum Exhibit C

Description of the Technical and Organisational 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 transmissio 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 protocol to encrypt all traffic in transit and Customer Data is securely encrypte 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 confidentialit obligations. Additionally, Company requires every downstrean Subprocessor to sign confidentiality provisions that are substantiall similar to those contained in Company's customer agreements. Company has undergone a SOC 2 Type 2 audit.
Measures for ensuring the ability to restore the availability and access to personal data in a timel manner in the event of a physical or technical incident	Supabase is Point-in-time: Database changes are logged every 2 minutes, with a total recovery period of up to 7 days. 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 has undergone a SOC 2 Type 2.
Measures for user identification and authorization	Company uses secure access protocols and processes and follows industry best-practices for authentication, including Multifactor Authentication, Least Privilege and RBAC. All production access requires the use of 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	Company has deployed secure methods and protocols for transmissio of confidential or sensitive information over public networks. Compan uses only recommended secure cipher suites and protocols to encryp all traffic in transit (i.e. TLS 1.2)

Measures for the protection of data during storage	Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.
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 tha process or store Customer Data, including cloud services. Monitoring o security logs is managed by the security and engineering teams. Lo 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 maintains a comprehensive security governance and I management framework designed to ensure organizational oversight policy enforcement, and continuous risk management. The framewor for Company's security program includes administrative organizational, technical, and physical safeguards reasonably designe to protect the Services and confidentiality, integrity, and availability o Customer Data.
Measures for certification/assurance of processes and products	Company undergoes annual SOC 2 Type II audits.
Measures for ensuring data minimization	Company's Customers unilaterally determine what data they route through the Services. As such, Company operates on a share responsibility model. Company gives Customers control over exactl what data enters the platform. Additionally, 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 and strong typing to enforce a strict contract between official clients and API resolvers. 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.

Data Processing Addendum 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 measure including technical and organisational measures t 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

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 t 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, whic is required by UK Data Protection Laws when you are making an ex-UK Transfer relying o 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 accordanc with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised unde Section 18 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission i Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data t countries not otherwise recognized as offering an adequate level of protection fo 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/o electronic communications in force from time to time in the UK, including the UK GDP 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 purposes 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 benefitting 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:

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

b) its risk under the UK Addendum,

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.