

# SLATE End-User License Agreement

Last updated: 03 April 2021

Authorized Users are subject to Customer's compliance with the SaaS License Agreement between the Provider and Customer which sets forth the necessary information relating to the Service that Customer has the right to receive and the fees payable for the Service.

By accessing and/or using the Services, including any updates, upgrades, or newer versions, Authorized User acknowledges having read and understood the linked Terms below in their entirety and agree to be legally bound by this End-User License Agreement (EULA). All graphics, user interfaces, data, processes, charts, flows and/or subject matter contained in the Service are the exclusive property of the Provider and no portions may be copied, screen shot, reproduced, uploaded, downloaded, printed, shown to, or shared in whole or in part with any third-party. Authorized User will not, in whole or in part, copy, distribute copies to any third party, modify, adapt, translate, reverse engineer, make alterations, decompile, disassemble, or make derivative works based on the Service. Some or all of Provider's Confidential and Proprietary Information may be entitled to further protection as a "trade secret", as the term is defined in the Uniform Trade Secrets Act (Civil Code 3426.1-11).

## 1. DEFINITIONS

- 1.1 Additional License Limitations means any Authorized User license limitations as set forth in the SaaS License Agreement with the Customer.
- 1.2 Authorized User means an individual designated by a Customer or Provider to receive a User ID, or account, to access the Service. The Customer or Provider are the entity affiliated with the Authorized User and the entity that provides the Authorized User the rights to access the Service.
- 1.3 Confidential Information means information of or relating to Provider or their respective affiliates, subsidiaries, suppliers, clients, customers or licensors, that is not generally known to the public, including without limitation, information that relates to past, present or future research and development, trade secrets, products and services, pricing, marketing, financial matters, or business affairs (including without limitation, policies, procedures, plans, methods of operation, specifications, manuals, programs, documentation, guidelines, procedures, forms, and report formats), systems, networks, computer equipment and software proprietary to or licensed by a party, including without limitation, object or source code, custom software modifications, software documentation and training aids, and all data, code, techniques, algorithms, methods, logic, architecture, and designs embodied or incorporated therein.
- 1.4 Consumer, for the purpose of the CCPA (California Consumer Privacy Act), means a natural person who is a California resident. A resident, as defined in the law, includes (1) every individual who is in the USA for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the USA who is outside the USA for a temporary or transitory purpose.
- 1.5 Cookies are small files that are placed on a computer, mobile device, or any other device by a website containing the details of a browsing session.
- 1.6 Customer Data means all documents, information, content, records, files, and data entered, received, processed, or stored by or for an Authorized User using the Service.
- 1.7 Data Law means any and all current and future laws, rules, regulations, and/or directives (whether foreign, federal, state or local) including those that protect Personal Data from unauthorized processing, disclosure, use, or reproduction, or that trigger a duty to notify an individual whose Personal Data has been, or may have been, the subject of unauthorized access or acquisition.
- 1.8 Device means any device that can access the Service such as a computer, a cellphone, or a digital tablet.
- 1.9 End-User License Agreement (EULA) This agreement between the Authorized Users and the Provider.
- 1.10 Personal Data means any Authorized User information that is capable of identifying a natural person, which may include but is not limited to: name, address, telephone number, e-mail address, social security number, national identification number, driver's license number; state-issued identification card number; and/or an

account number, in combination with or without any required security code, access code or password that would permit access to an individual's account. "Personal Data" also includes any other data, such as, but not limited to, identifiers, including biometric identifiers, demographic, or behavioral data, when such data, either alone or in combination with other data identifies or has the capacity of identifying, a specific person.

- 1.11 Privacy Policy means the conditions established in "Privacy Policy" (below) in this EULA, as may be modified from time to time.
- 1.12 Protected Data means any Personal Data, and any other information that is protected by any applicable Data Law, which is provided to the Provider by or at the direction of Customer, created or obtained by the Provider on behalf of Customer, or is information to which access was provided to Provider by or at the direction of Customer, in the course of providing the Services.
- 1.13 Provider means Energy Project Systems, Inc. (EPS) of Maricopa County in the State of Arizona, USA, or its Licensees.
- 1.14 Provider Personnel means all personnel furnished or engaged by the Provider to assist in performance under this Agreement (including obligations under this Policy), including, officers, employees, representatives, and agents of the Provider and permitted subcontractors.
- 1.15 Registration Information means the information provided by individual Authorized Users to access and use the Service.
- 1.16 SaaS License Agreement means agreement between Provider and its Customers (not the Authorized User).
- 1.17 Sale, for the purpose of the CCPA (California Consumer Privacy Act), means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Consumer's Personal Data to another business or a third party for monetary or other valuable consideration.
- 1.18 Service (SaaS) means Provider's proprietary Software-as-a-Service (SaaS) platform known as SLATE that runs complex tablet-based campaigns and creates real-time actionable business intelligence level information from the data, where such platform is accessed and used by Authorized Users on a service basis via the internet or private network.
- 1.19 Security Incident means the occurrence of any act or omission that compromises the confidentiality, integrity, or availability of Protected Data or the physical, technical, administrative, or organizational safeguards put in place by the Provider that relate to the protection of the confidentiality, integrity, or availability of Protected Data, including without limitation any circumstance pursuant to which applicable Data Law requires notification of such incident to be given to affected parties or other activity in response to such circumstance.
- 1.20 System Requirements means collectively, the hardware, software, network, and internet access required for Authorized User to access the Service.
- 1.21 Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).
- 1.22 User ID means a unique user identification in the Service of an Authorized User.

## **2. SERVICE PLATFORM**

- 2.1 License. Subject to compliance with this Agreement, including any Additional License Limitations, EPS hereby grants to Authorized User a non-exclusive, personal, and non-transferable license, during the term of the applicable SaaS License Agreement, to access and use the Service solely for Customer or Provider business use.
- 2.2 Restrictions. Except as expressly set forth herein, Authorized User will not, in whole or in part: copy the Service, disclose, or distribute copies of the Service to any third party; modify, adapt, translate, reverse engineer, make alterations, decompile, disassemble or make derivative works based on the Service except as otherwise permitted by law; rent, loan, sub-license, lease, distribute or attempt to grant any rights to the Service to third parties; use the Service to act as a service bureau, or to permit access to the Customer Data by any kind to any third-party; or remove, alter, or obscure any proprietary notice (including any notice of copyright or trademark) of EPS or its affiliates, customers, partners, suppliers, or the licensors of the Service.

### **3. SERVICE AVAILABILITY**

- 3.1 Service Availability. The Service shall be available 24 hours a day, 7 days a week, 365 days a year, excluding periods of routine maintenance checks (“Scheduled Maintenance”) or emergency maintenance (“Emergency Maintenance”). Provider agrees to post a notice to Authorized Users on the Service at least 24 hours in advance for Scheduled Maintenance outside of normal business hours and will use commercially reasonable efforts to perform Scheduled Maintenance outside of regular business hours.
- 3.2 Authorized User Access. The Service is to be accessed for field-based activities during site working hours as established by the Customer and Provider, as may be modified from time to time.
- 3.3 Modifications to Service. The Provider reserves the right to modify, suspend, or discontinue, temporarily or permanently, the Service or any service to which it connects, with or without notice and without liability to any Authorized User. The Provider may from time to time provide enhancements or improvements to the features/functionality of the Service, which may include patches, bug fixes, updates, upgrades, and other modifications. Updates may modify or delete certain features and/or functionalities of the Service. The Authorized User agrees the Provider has no obligation to provide any updates or continue to provide or enable any particular features and/or functionalities of the Service, and that all updates or any other modifications will be deemed to constitute an integral part of the Service and be subject to the terms and conditions of this EULA.

### **4. AUTHORIZED USER RESPONSIBILITIES**

- 4.1 Registration Information and User IDs. Each Authorized User will have a unique User ID for his or her access to the Service. Authorized Users will use only their respective assigned User IDs and will never use another’s User ID. Authorized Users will adopt and maintain such security precautions for User IDs to prevent their disclosure to and use by unauthorized persons and will promptly notify the Provider if the security or integrity of a User ID or password has been compromised.
- 4.2 Authorization; Noninfringement; Delivery of Customer Data. Authorized Users are responsible for obtaining all authorizations, consents, releases, and permissions necessary or desirable to enter Customer Data into the Service, to use the Service to process and store Customer Data, and to receive the Services. Authorized Users will not submit any Customer Data or use the Services in any way that infringes, misappropriates, or violates any trademark, copyright, patent, trade secret, publicity, privacy, or other right of any third party or violates any applicable local, state, or federal laws, statutes, ordinances, rules, or regulations or any judicial or administrative orders. Provider shall not be liable for the accuracy, completeness, or authenticity of Customer Data furnished by Authorized User or any other third party, and shall have no obligation or responsibility to audit, check or verify the Customer Data. Authorized User shall transmit and receive Customer Data by means of a secure network connection with Provider. Any transmission method used must conform to Provider’s specifications and requirements. Provider shall not be liable or responsible for any loss or delay of Customer Data, reports or any other information that pertains to Customer or the Services during any period of transit or electronic transmission to or from Provider’s facility or other agreed delivery location if through no fault of Provider.
- 4.3 No Interference with Service Operations. Authorized User will not take any action that: interferes or attempts to interfere with the proper working of the Service or engage in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of the Service; circumvents, disables, or interferes or attempts to circumvent, disable, or interfere with security-related features of the Service or features that prevent or restrict use, access to, or copying of any data or enforce limitations on use of the Service or data; or imposes or may impose, in Provider’s sole discretion, an unreasonable or disproportionately large load on the Service infrastructure.
- 4.4 Authorized User Review and Responsibility. Authorized User will be solely responsible for any services that it provides to others involving the use of the Service, Customer Data, or the Services. Provider makes no representations concerning the completeness, accuracy, or utility of any Customer Data in the Service, or any qualifications or competence of anyone that may place Customer Data in the Service. Authorized Users shall be solely responsible for ensuring accuracy, completeness and compliance of any Customer Data provided to any third-party, and all liabilities and responsibilities in connection with such Customer Data. Provider shall not be responsible for the accuracy, completeness, or compliance thereof. Neither Authorized Users nor any other

person will have any claim or cause of action against Provider as a result of any professional or other services rendered or withheld in connection with the use of the Service.

- 4.5 Content Restrictions. Provider is not responsible for the entries, information, or content of the Authorized User. The Authorized User expressly understands and agrees to being solely responsible for the content and for all activity that occurs with an assigned User ID, whether done so by Authorized User or any third person using an Authorized Users account. Authorized User may not transmit any content that is unlawful, offensive, upsetting, intended to disgust, threatening, libelous, defamatory, obscene, or otherwise objectionable. Examples of such objectionable content include, but are not limited to, the following: unlawful or promoting unlawful activity; defamatory, discriminatory, or mean-spirited content, including references or commentary about religion, race, sexual orientation, gender, national/ethnic origin, or other targeted groups; spam, machine – or - or randomly - – generated, constituting unauthorized or unsolicited advertising, chain letters, any other form of unauthorized solicitation, or any form of lottery or gambling; containing or installing any viruses, worms, malware, trojan horses, or other content that is designed or intended to disrupt, damage, or limit the functioning of any software, hardware or telecommunications equipment or to damage or obtain unauthorized access to any data or other information of a third person; or impersonating any person or entity including the Provider and its employees or representatives.
- 4.6 Content Review. The Provider reserves the right, but not the obligation, to, in its sole discretion, determine whether or not any content is appropriate and complies with this EULA, and may refuse or remove any content. The Provider further reserves the right to make formatting and edits and change the manner any content. The Provider can also limit or revoke the use of the Service if Authorized User post such objectionable content. As the Provider cannot control all content posted by users and/or third parties on the Service, you agree to use the Service at your own risk. Authorized User understand that by using the Service, Authorized User may be exposed to content that Authorized User may find offensive, indecent, incorrect, or objectionable, and Authorized User agrees that under no circumstances will the Provider be liable in any way for any content, including any errors or omissions in any content, or any loss or damage of any kind incurred as a result of your content use.

## 5. TERMINATION

- 5.1 This EULA shall begin upon Authorized User’s initial access to the Services and remain in effect until access is restricted, suspended or terminated by Provider. Provider will have the right to restrict, suspend or terminate access upon thirty (30) days prior written notice if the Authorized User is in material breach of this EULA or Customer is in breach of or terminates the applicable SaaS License Agreement, and the breaching party fails to remedy such breach within such notice period. Notwithstanding the foregoing, Provider may immediately terminate access to the Service upon written notice to the Authorized User if the Authorized User violates the scope or any restriction on its license or its obligations hereunder with respect to Confidential Information.
- 5.2 Effect of Termination. Upon termination for any reason, all licenses granted hereunder will automatically terminate, and Provider may immediately disable and discontinue Authorized User’s access to and use of the Service without additional notice to the Authorized User. Authorized User will return to Provider all materials it has acquired pertaining to the Service or any Confidential Information.

All rights to any provisions of this EULA which by their nature are intended to survive termination will survive any expiration or termination of the EULA, including the Provider's rights or remedies at law or in equity in case of breach by Authorized User (during the term of this EULA) of any of your obligations under the present EULA.

## 6. PROPRIETARY RIGHTS; OWNERSHIP

- 6.1 Service. Provider is and will remain the exclusive owner of all right, title and interest in and to the Service, any updates, modifications or upgrades thereto, Provider’s Confidential Information, and all other specifications, manuals, tapes, programs, documentation, reports, systems, work product and/or other tangible or intangible material of any nature developed or provided by Provider or otherwise accessible to the Authorized User or any feedback provided by the Authorized User in connection with the provision of any Services under this EULA, including all intellectual property rights therein (“Provider Materials”). Authorized User hereby acknowledges and agrees that the Provider Materials, including without limitation, its Confidential Information, constitute and

contain valuable proprietary products and trade secrets of Provider, embodying substantial creative efforts and confidential information, ideas, and expressions. Authorized User agrees to assign, and hereby assigns, all right, title and interest to any feedback, derivative works, or improvements to the Services to Provider.

- 6.2 Customer Data. To the extent Authorized User retains any rights to Customer Data, Authorized User grants to Provider a non-exclusive license, during the term of this EULA, to use, reproduce, modify, display, and distribute Customer Data for the purposes of performing its obligations under this EULA. Subject to the foregoing, Customer is and will remain the owner of all right, title and interest in and to all Customer Data and Customer Confidential Information.
- 6.3 Aggregated Information. Authorized User acknowledges and agrees that all general, anonymized or otherwise aggregated information based on Customer Data from Authorized User's use of the Services or data based on Authorized User's overall use of the Services ("Aggregated Statistics") are and will remain the property of Provider. Authorized Users agree that Provider may make Aggregated Statistics publicly available in compliance with applicable law, and use Aggregated Statistics to the extent and in the manner permitted under applicable law, provided that such Aggregated Statistics do not identify Customer, any Authorized User or Customer's Confidential Information. To the extent Authorized User retains any rights to Customer Data, Authorized User hereby grants to Provider a non-exclusive, royalty-free, perpetual, worldwide license to access, revise, reproduce, distribute, and use and display Customer Data incorporated within the Aggregated Statistics.
- 6.4 Feedback. To the extent that Provider receives from Authorized User any suggestions, ideas, improvements, modifications, feedback, error identification, or other information related to the Service or any other products or services ("Feedback"), Provider may use, copy, modify, publish, disclose, and exploit such Feedback without restriction or compensation, including to improve the Services and to develop, market, offer, sell, and provide other products and services.

## **7. CONFIDENTIAL INFORMATION AND PRIVACY**

- 7.1 Obligations. The parties acknowledge that the Services require disclosure by each party ("Disclosing Party") to the other party ("Receiving Party") of certain of the Disclosing Party's Confidential Information. With respect to Confidential Information of the Disclosing Party that is disclosed to the Receiving Party, the Receiving Party shall, subject to the exceptions stated herein: (a) maintain and protect the confidentiality of the information with the same care and measures to avoid unauthorized disclosure or access as the Receiving Party uses with its own Confidential Information, but in no event less than a reasonable standard of care; (b) use the information solely to carry out the purposes for which the information was disclosed; and limit access to the information to: (i) employees of the Receiving Party, or of its subsidiaries or affiliates, who have a need to know to facilitate, monitor or review the delivery, receipt or performance of the Services; (ii) employees of the Receiving Party's suppliers or licensors who have a need to know the information solely for the purpose of facilitating the performance, delivery or use of the Services; and (iii) the Receiving Party's external attorneys and auditors. Any of the foregoing individuals to whom the Receiving Party discloses information must be under a legally binding obligation to maintain the confidentiality of the information. The Receiving Party shall remain responsible to the Disclosing Party for acts or omissions of such individuals that if committed by the Receiving Party would constitute a violation of the Receiving Party's confidentiality obligations hereunder. Customer or any of its Authorized Users shall not disclose the terms and conditions of this EULA, including without limitation, pricing, to any third party without Provider's prior written consent.
- 7.2 Exceptions. The Receiving Party shall not be in violation of this EULA for: (a) disclosing Confidential Information of the Disclosing Party that (i) is or becomes publicly available other than as a result of a breach of this EULA, (ii) is disclosed to the Receiving Party by a third party not subject to any obligation of confidentiality, (iii) was already known by the Receiving Party prior to the date of this EULA (unless disclosed in connection with negotiations and discussions related to this EULA or associated transactions), or (iv) was independently developed by the Receiving Party without reference to Confidential Information received from the Disclosing Party; or (b) disclosing Confidential Information of the Disclosing Party when required to do so by (i) the Receiving Party's federal or state regulatory agencies, or (ii) a federal or state law or regulation, or a subpoena or court order or agency action that requires disclosure, provided, however, that, if disclosure of Confidential Information is required by any of the foregoing, the Receiving Party shall, unless prohibited by law,

regulation or court or agency order, promptly notify the Disclosing Party and, at the Disclosing Party's request and expense, cooperate with the Disclosing Party's efforts, if any, to prevent or limit the disclosure.

- 7.3 No License; Return of Information. Nothing in this Section shall be construed as a grant or assignment of any right or license in the Disclosing Party's Confidential Information. The Disclosing Party's Confidential Information shall at all times remain the property of the Disclosing Party. At any time the Disclosing Party may reasonably request, and in any event upon the termination or expiration of this EULA, the Receiving Party shall, at the election of the Disclosing Party, promptly return to the Disclosing Party all Confidential Information of the Disclosing Party in the Receiving Party's possession or control, or certify in writing to the Disclosing Party that the Confidential Information has been destroyed, subject to any provisions in this EULA regarding return of Customer's Data or as otherwise agreed between the parties for the transfer of Customer's Data to a third party.
- 7.4 Remedies and Responsibilities. The Receiving Party acknowledges that the Disclosing Party has the right to take all reasonable steps to protect the Disclosing Party's Confidential Information, including without limitation, seeking injunctive relief and/or any other remedies that may be available at law or in equity, all of which remedies shall be cumulative and in addition to any rights and remedies available by contract, law, rule, regulation or order. Any requirements for a bond in connection with any such injunctive or other equitable relief are hereby waived by both parties.
- 7.5 Privacy Policy. Provider is bound by its Privacy Policy which governs the collection, processing and use of Confidential Information and data. The Privacy Policy is updated regularly to accommodate changes in legislation with respect to Confidential Information which may be accessible to either party in carrying out their respective obligations under this EULA. Customer Data shall be treated as Confidential Information under this EULA.

## **8. WARRANTY; LIMITATIONS AND DISCLAIMER**

- 8.1 Warranty. The Provider does not make any warranties concerning the Service. Provider will not be responsible or liable with respect to any problems or issues arising from unauthorized or improper use of the Service; modification, alteration or configuration of the Service by or for Authorized User that has not been authorized in writing by Provider; hardware, software, technology or intellectual property which has not been provided by Provider pursuant to this EULA; communications facilities; any breach of this EULA by Authorized User, or any act or omission of any Authorized User which, if performed or omitted by Authorized User would be a material breach of this EULA; and/or failure to comply with System Requirements including any act or omission of Authorized User that prevents, delays, disturbs or interferes with Provider's performance of its obligations hereunder.
- 8.2 Service Limitations. The Service may be temporarily unavailable from time to time due to required maintenance, telecommunications interruptions, or other disruptions. Provider may also make improvements and/or changes in the Service at any time without notice. Provider will not be responsible for any damages that Authorized User may suffer arising out of use, or inability to use, the Service. Provider will not be liable for unauthorized access to or alteration, theft or destruction of Authorized User's data files, programs, procedures or information through accident, fraudulent means or devices, or any other method. It is hereby acknowledged that it is Authorized User's responsibility to validate Customer Data for correctness and to protect Customer's Data from loss by maintaining back-ups of all Customer Data and routinely updating such back-ups. Authorized User hereby waives any damages occasioned by incorrect, lost, or corrupt Customer Data, or incorrect data files resulting from a programming error, operator error, equipment, or software malfunction, or from the use of third-party software.
- 8.3 Disclaimer of Warranties. EXCEPT AS EXPRESSLY PROVIDED HEREIN, PROVIDER MAKES NO OTHER WARRANTIES RELATED TO THE SERVICES PROVIDED BY PROVIDER HEREUNDER, AND HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. AUTHORIZED USER ASSUMES TOTAL RESPONSIBILITY FOR THE SELECTION OF THE SERVICES TO ACHIEVE AUTHORIZED USER'S INTENDED RESULTS AND FOR ITS USE OF THE RESULTS OBTAINED FROM THE SERVICES. PROVIDER DOES NOT WARRANT THAT THE SERVICES MEET AUTHORIZED USER'S REQUIREMENTS OR WILL BE UNINTERRUPTED OR ERROR FREE.

8.4 Limitations of Liability. IN NO EVENT WILL PROVIDER (INCLUDING ITS SUBSIDIARIES, ITS PARENT AND SUBSIDIARIES OF ITS PARENT, ITS SERVICE PROVIDERS AND LICENSORS, AND THE EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS THEREOF) BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR PUNITIVE DAMAGES UNDER THIS EULA OR IN CONNECTION WITH ANY SERVICES PROVIDED BY PROVIDER HEREUNDER, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE SERVICES, DATA, EVEN IF PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF AVAILABLE REMEDIES ARE FOUND TO HAVE FAILED THEIR ESSENTIAL PURPOSE. THE TOTAL LIABILITY, IF ANY, OF PROVIDER (INCLUDING ITS SUBSIDIARIES, ITS PARENT AND SUBSIDIARIES OF ITS PARENT, ITS SERVICE PROVIDERS AND LICENSORS, AND THE EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS THEREOF) IN THE AGGREGATE OVER THE TERM OF THIS EULA FOR ALL CLAIMS, CAUSES OF ACTION OR LIABILITY WHETHER SOUNDING IN CONTRACT, TORT OR OTHERWISE ARISING UNDER OR IN ANY WAY RELATED TO THIS EULA AND/OR THE SERVICES PROVIDED HEREUNDER (COLLECTIVELY, "CLAIMS"), SHALL BE LIMITED TO THE LESSER OF: (A) AUTHORIZED USER'S DIRECT DAMAGES, ACTUALLY INCURRED, OR (B) THE TOTAL FEES PAID BY CUSTOMER TO PROVIDER IN THE MOST RECENT THREE (3) MONTH PERIOD. NOTWITHSTANDING THE FOREGOING, PROVIDER'S SOLE OBLIGATION IN THE EVENT OF AN ERROR BY PROVIDER IN THE PERFORMANCE OF ANY SERVICES UNDER THIS EULA SHALL BE LIMITED TO REPROCESSING APPLICABLE DATA OR REPERFORMING THE SERVICES. PROVIDER (INCLUDING ITS SUBSIDIARIES, ITS PARENT AND SUBSIDIARIES OF ITS PARENT, ITS SERVICE PROVIDERS AND LICENSORS, AND THE EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS THEREOF) SHALL HAVE NO LIABILITY, EXPRESS OR IMPLIED, WHETHER ARISING UNDER CONTRACT, TORT OR OTHERWISE, FOR ANY CLAIM OR DEMAND: (A) RESULTING DIRECTLY OR INDIRECTLY FROM AUTHORIZED USER'S EQUIPMENT, SYSTEMS OR SOFTWARE OWNED OR LICENSED BY AUTHORIZED USER; OR (B) BY THIRD PARTIES, EVEN IF PROVIDER WAS ADVISED OF THE POSSIBILITY OF SUCH CLAIMS OR DEMANDS, EXCEPT AS EXPRESSLY OTHERWISE PROVIDED HEREIN.

## 9. INDEMNIFICATION

- 9.1 Indemnification of Provider by Authorized User. Authorized User shall indemnify and hold harmless Provider, its officers, agents, employees, affiliates, subsidiaries, assigns and successors in interest from, defend Provider against, pay any final judgments awarded against Provider, and pay all of Provider's reasonable costs and attorneys' fees resulting from any claims, liabilities, losses, suits, and damages asserted by a third party based on: Authorized User's improper or misuse of the Services (including without limitation, in violation of applicable laws, rules or regulations or this EULA); Provider's compliance with Authorized User's instructions; Provider's use of trademarks, Customer Data or other materials supplied by Authorized User; Any breach or alleged breach by Authorized User of this EULA; The conduct of any business in connection with use of the Services; or alleged infringement of any patent, copyright, trademark, trade secret, or other intellectual property or proprietary rights of a third party arising out of any Authorized User content, materials or software.
- 9.2 Indemnification Procedures. If any third party makes a claim against an indemnitee with respect to which such indemnitee intends to seek indemnification under this Section, such indemnitee shall give notice of such claim to the indemnifying party, including a brief description of the amount and basis therefor, if known. Upon giving such notice, the indemnifying party shall be obligated to defend such indemnitee against such claim, and shall be entitled to assume control of the defense of the claim with counsel chosen by the indemnifying party, reasonably satisfactory to the indemnitee. The indemnitee shall cooperate fully with and assist the indemnifying party in its defense against such claim in all reasonable respects. The indemnifying party shall keep the indemnitee fully apprised at all times as to the status of the defense. Notwithstanding the foregoing, the indemnitee shall have the right to employ its own separate counsel in any such action, but the fees and expenses of such counsel shall be at the expense of the indemnitee. Neither the indemnifying party nor any indemnitee shall be liable for any settlement of action or claim effected without its consent. Notwithstanding the foregoing, the indemnitee shall retain, assume, or reassume sole control over all expenses relating to every aspect of the defense that it believes is not the subject of the indemnification provided for in this Section. Until both the

indemnitee receives notice from indemnifying party that it will defend, and the indemnifying party assumes such defense, the indemnitee may, at any time after ten (10) days from the date notice of claim is given to the indemnifying party by the indemnitee, resist or otherwise defend the claim or, after consultation with and consent of the indemnifying party, settle or otherwise compromise or pay the claim. The indemnitee shall keep the indemnifying party fully apprised at all times as to the status of the defense.

## 10. GENERAL

- 10.1 Assignment, Successors. No right or license under this EULA may be assigned or transferred by Authorized User, nor may any duty be delegated by Authorized User without Provider's prior written consent. Any assignment, transfer, or delegation in contradiction of this provision will be null and void. Subject to the foregoing, this EULA will bind and inure to the benefit of the successors and assigns of Provider.
- 10.2 Subcontracting. Provider may freely subcontract its duties and obligations under this EULA. In the event that Provider subcontracts any of its duties and obligations, Provider agrees that: the third party shall execute a confidentiality agreement consistent with the terms of this EULA, and any such permitted subcontracting shall not release Provider from any of its obligations under this EULA.
- 10.3 Force Majeure. Notwithstanding any other provision of this EULA, no party to this EULA shall be deemed in default or breach of this EULA or liable for any loss or damages or for any delay or failure in performance (except for the payment of money) due to any cause beyond the reasonable control of, and without fault or negligence by, such party or its officers, directors, employees, agents, or contractors. Without limiting the foregoing, the following shall constitute events of force majeure: acts of State or governmental action, riots, war, terrorism, strikes, lockouts, prolonged shortage of energy supplies, epidemics, fire, flood, hurricane, typhoon, earthquake, lightning, explosion, any other acts of God or any third party, the failure of telecommunications equipment or other hardware, any third-party software, or any third-party services.
- 10.4 Governing Law. This EULA shall be governed by the laws of the State of Arizona, excluding its principles of conflicts of laws. Any dispute shall be litigated in the federal courts located in Maricopa County, Arizona, to whose jurisdiction the parties hereby consent.
- 10.5 Notice. All notices required or permitted under this EULA and Privacy Policy will be in writing and sent by certified mail, return receipt requested, or by reputable oversight courier, or by hand delivery. The notice address for Provider is 14362 N Frank L Wright Blvd, Suite 1000, Scottsdale, AZ 85260, or using the Contact form on the [www.eps-inc.co](http://www.eps-inc.co) website or at [info@eps-inc.co](mailto:info@eps-inc.co).
- 10.6 Independent Contractor. Provider is acting as an independent contractor in its capacity under this EULA. Nothing contained in this EULA or in the relationship of the Authorized User and Provider shall be deemed to constitute a partnership, joint venture, or any other relationship between the Authorized User and Provider except as is limited by the terms of this EULA.
- 10.7 Miscellaneous. This EULA, together with the exhibits hereto, constitutes the entire agreement between Provider and Authorized User with respect to the subject matter hereof. There are no restrictions, promises, warranties, covenants, or undertakings other than those expressly set forth herein and therein. This EULA supersedes all prior negotiations, agreements, and undertakings between the parties with respect to such matter. This EULA, including the exhibits hereto, may be amended only by an instrument in writing executed by the parties or their permitted assignees. No provision of this EULA shall be construed against or interpreted to the disadvantage of any party hereto by any court or arbitrator by reason of such party having or being deemed to have structured or drafted such provision. The headings in this EULA are for reference purposes only and shall not be deemed to have any substantive effect. If any provision of this EULA is held by a court or arbitrator of competent jurisdiction to be contrary to law, then the remaining provisions of this EULA will remain in full force and effect. The failure of either party at any time to require performance by the other party of any provision of this EULA shall not affect in any way the full right to require the performance at any subsequent time. The waiver by either party of a breach of any provision of this EULA shall not be taken or held to be a waiver of the provision itself. Any course of performance shall not be deemed to amend or limit any provision of this EULA. This EULA may be signed in counterparts with the same effect as if the signatures were upon a single instrument, and all such counterparts together shall be deemed an original of this EULA. For purposes of this EULA, an electronic or facsimile copy of a party's signature shall be sufficient to bind such party.



## Appendix 1 - Privacy Policy

This Privacy Policy describes the policies and procedures on the collection, use, and disclosure of Authorized User information when using the Service and how privacy rights are protected by the Provider. The Provider uses Personal Data to deliver and improve the Service. By using the Service, the Authorized User agrees to the collection and use of information in accordance with this Privacy Policy.

### 1. ACCESS TO PROTECTED DATA

- 1.1 Applicability. In the performance of the EULA, the Provider might receive or be granted access to Protected Data from time to time. This Policy stipulates the Provider's obligations in respect to this Protected Data.
- 1.2 Compliance with Laws. Provider and Customer shall comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this Policy, including all applicable Data Law. If a party believes that performance by either party under this Policy or the agreement will violate applicable Data Law, then such party shall immediately notify the other party. Upon a party's written request, the other party shall provide information as necessary for the requesting party to comply with any applicable Data Law. The parties shall cooperate in good faith with such inquiries. Each party shall treat any Protected Data provided by the other party as the other party's Confidential Information.
- 1.3 Restrictions on Provider's Receipt, Use, and Disclosure of Protected Data. To the extent Provider has access to or collects Protected Data, it shall use and disclose Protected Data solely in connection with performance under this EULA and as permitted under this Policy (except to the extent otherwise specifically required by applicable Data Law) and shall not otherwise disclose Protected Data to any third-party. Provider shall maintain the confidentiality of Protected Data and shall treat it in accordance with this EULA and applicable Data Law.

### 2. PERSONAL DATA (TYPES COLLECTED)

- 2.1 Personal Data. While using the Services, certain personally identifiable information that may be collected which may include, but is not limited to email address, first name, and last name, phone number, and Usage Data.
- 2.2 Usage Data. Usage Data is collected automatically when using the Service. Usage Data may include information such as a Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service visited, the time and date visited, the time spent on those pages, unique device identifiers and other diagnostic data. When accessing the Service by or through a mobile device, the Service may collect certain information automatically, including, but not limited to, the type of mobile device, mobile device unique ID, the IP address, mobile device operating system, the type of internet browser used, unique device identifiers, diagnostic data, and information the browser sends when accessing the Service.
- 2.3 Tracking Technologies and Cookies. Cookies and similar tracking technologies are used to track activity and store certain information during access to the Service. Tracking technologies used may include beacons, tags, and scripts to collect and track information and to improve and analyze the Service. The Authorized User may instruct the browser to refuse all Cookies or to indicate when a Cookie is being sent. However, Cookies are an essential part of the Service and restricting Cookie use likely create user experience problems and parts of the Service may not function properly. Unless the Authorized User browser setting refuse Cookies, the Service will use Cookies. Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on a personal computer or mobile device when offline, while Session Cookies are deleted as soon as the web browser is closed.

The Service places and administers both Session and Persistent Cookies for the purposes set out below:

- **Necessary / Essential Cookies [Session Cookies: Yes]**  
Purpose: These Cookies are essential to provide the Service through a web browser and perform all the features. They help to authenticate users and prevent fraudulent account use. Without these Cookies, the Services cannot be provided, and these Cookies are only used to provide the Services.
- **Cookies Policy / Notice Acceptance Cookies [Persistent Cookies: Yes]**  
Purpose: These Cookies identify if Authorized Users have accepted the use of cookies on the Website.

- **Functionality Cookies [Persistent Cookies: Yes]**

Purpose: These Cookies allow us to remember Authorized User choices when using the Service, such as remembering login details or language preference. The purpose of these Cookies is to provide a more personal experience and to avoid having to re-enter your preferences every time a new page is loaded.

### 3. PERSONAL DATA (USES)

- 3.1 Provide the Service. Includes monitoring, maintenance, and Service use.
- 3.2 Account Management: Authorized User registration where the Personal Data provided provides access to different functionalities of the Service.
- 3.3 Contract Performance: The development, compliance, and undertaking of the purchase contract for the Services.
- 3.4 Authorized User Contact: To contact by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, enhancements, and the security updates.
- 3.5 Authorized User Requests: To attend and manage requests, service bugs, and other similar communication.
- 3.6 Other Purposes: Personal Data may be used for other purposes such as data analysis, identifying usage trends, determining the effectiveness of campaigns, and to evaluate and improve the services, marketing, and user experience.

### 4. PERSONAL DATA (SHARING)

- 4.1 With Service Providers: Provider may share Authorized User Personal Data with third-party service providers that monitor and analyze Service usage, to contact Authorized User.
- 4.2 For Business Transfers: Provider may share or transfer Personal Data in connection with, or during negotiations of, any merger, sale of Provider assets, financing, or acquisition of all or a portion of the Providers business to another company.
- 4.3 With Affiliates: Provider may share Authorized User information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent Provider and any other subsidiaries, joint venture partners or other companies that Provider control or that are under common control with Us.
- 4.4 With Business Partners: Provider may share Authorized User information with Provider business partners to offer Authorized User certain products, services, or promotions.
- 4.5 With Other Users: When Authorized User shares Personal Data or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside. If Authorized User interact with other users or registers through a third-party social media service, Authorized User contacts may see names, profile, pictures, and description of Authorized User activity. Similarly, other users will be able to view descriptions of Authorized User activity, communicate with Authorized User, and view Authorized User profile.
- 4.6 Authorized User Consent: Provider may disclose Authorized User Personal Data for any other purpose with Authorized User consent.
- 4.7 Provider Personnel and Subcontractors: Provider shall cause all Provider Personnel to whom Provider provides, permits access to, or allows to use Protected Data, to agree to the same restrictions and conditions that apply to Provider under this Policy. Customer agrees that Provider may use third parties to fulfill any or all of its obligations under this Policy. If required by applicable Data Law, Provider will provide Customer with a list identifying the third parties that are authorized by Provider to have access to Protected Data, inform Customer of any changes to those third parties, and provide Customer with a period of time before such changes go into effect during which to notify Provider of Customer's objections, if any, to such changes.

## **5. PERSONAL DATA PROCESSING**

The Service may contain links to other websites that are not operated by the Provider. If Authorized User click on a third-party link, Authorized User may be directed to that third party's site. These third-party vendors collect, store, use, process, and transfer information about Authorized User activity in accordance with their Privacy Policies. Provider strongly advise Authorized User to review the Privacy Policy of every site Authorized User visits.

Provider have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

## **6. PERSONAL DATA RETENTION**

The Provider will retain Authorized User Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. Provider will retain and use Authorized User Personal Data to the extent necessary to comply with any legal obligations (for example, if required to retain data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Provider will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of the Service, or Provider is legally obligated to retain this data for longer time periods.

## **7. PERSONAL DATA TRANSFER**

Authorized User information, including Personal Data, is processed at the Provider's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to, and maintained on, computers located outside of Authorized User state, province, country, or other governmental jurisdiction where the data protection laws may differ than those from Authorized User jurisdiction.

Authorized User consent to this Privacy Policy followed by Authorized User submission of such information represents Authorized User agreement to that transfer.

The Provider will take all steps reasonably necessary to ensure that Authorized User data is treated securely and in accordance with this Privacy Policy and no transfer of Authorized User Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Authorized User Personal Data.

## **8. PERSONAL DATA DISCLOSURE**

- 8.1 Business Transactions - If the Provider is involved in a merger, acquisition or asset sale, Personal Data may be transferred. Provider will provide notice before Authorized User Personal Data is transferred and becomes subject to a different Privacy Policy.
- 8.2 Law Enforcement - Under certain circumstances, the Provider may be required to disclose Authorized User Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).
- 8.3 Other Legal Requirements - The Provider may disclose Authorized User Personal Data in the good faith belief that such action is necessary to: Comply with a legal obligation, protect and defend the rights or property of the Provider, prevent or investigate possible wrongdoing in connection with the Service, protect the personal safety of Users of the Service or the public, and protect against legal liability.

## **9. PERSONAL DATA SECURITY**

The security of Authorized User data is important but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While Provider strives to use commercially acceptable means to protect Authorized User Personal Data, Provider cannot guarantee its absolute security.

In the event of a Security Incident, Provider shall notify Customer as soon as practicable, and within the maximum period allowed by applicable Data Law, after Provider becomes aware of the Security Incident. Provider shall take commercially reasonable steps to remedy the breach in accordance with applicable Data Law, and any other actions in Provider's discretion to ensure that similar Security Incidents do not recur.

Provider shall provide reasonable assistance and cooperation to Customer in investigating, remedying, and taking any other action Customer deems necessary regarding any Security Incident and any dispute, inquiry or claim that concerns the Security Incident and shall cooperate with any law enforcement or regulatory official investigating such Security Incident. Notwithstanding the foregoing, Provider's obligation to report or respond to a Security Incident under this Section is not an acknowledgement by Provider of any fault or liability of Provider with respect to the Security Incident.

## **10. PERSONAL DATA RETURN OR DESTRUCTION**

At Customer's request upon termination or expiration of this EULA for any reason, and subject to requirements of applicable Data Law, Provider shall instruct all Provider personnel to return to Customer all copies, whether in written, electronic, or other form or media, of Protected Data in its possession or the possession of such Provider personnel, or securely dispose of all such copies, and certify in writing to Customer that all such Protected Data, in all formats, including paper, electronic and disk form, has been returned, deleted, destroyed or rendered unreadable. For clarity, and notwithstanding the foregoing, Provider may retain Protected Data to the extent necessary to comply with applicable Data Law.

## **11. CHILDREN'S PRIVACY**

The Service does not knowingly collect or sell Personal Data from minors under the age of 16, although certain third-party websites that link to the Service may do so. These third-party websites have their own terms of use and privacy policies and we encourage parents and legal guardians to monitor their children's internet usage and instruct their children to never provide information on other websites without their permission.

If Authorized User have reason to believe that a child under the age of 16 has gained access to the Service as an Authorized User, and provided Personal Data, please contact the Provider with sufficient detail to enable that information to be deleted.

## **12. CALIFORNIA RESIDENTS (CCPA PRIVACY)**

This privacy notice section for California residents supplements the information contained in this Privacy Policy and it applies solely to all visitors, Authorized Users, and others who reside in the State of California.

- 12.1 Categories of Personal Information Collected. The Service collects information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Authorized User or Device. The following is a list of categories of Personal Data which may be collected or may have been collected from California residents within the last twelve (12) months. Please note that the categories and examples provided in the list below are those defined in the CCPA. This does not mean that all examples of that category of Personal Data were in fact collected by the Provider but reflects our good faith belief to the best of our knowledge that some of that information from the applicable category may be and may have been collected. For example, certain categories of Personal Data would only be collected if Authorized User directly provided such Personal Data.

### **Category A: Identifiers [Collected: Yes]**

Examples: A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, driver's license number, passport number, or other similar identifiers.

### **Category B: California Customer Records (Cal. Civ. Code § 1798.80(e)). [Collected: No]**

Examples: A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some Personal Data included in this category may overlap with other categories.

### **Category C: California or Federal law Protected Classification [Collected: No]**

Examples: Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).

**Category D: Commercial information. [Collected: No]**

Examples: Records and history of products or services purchased or considered.

**Category E: Biometric information. [Collected: No]**

Examples: Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.

**Category F: Internet or other similar network activity. [Collected: Yes]**

Examples: Interaction with our Service or advertisement.

**Category G: Geolocation data. [Collected: Yes]**

Examples: Approximate physical location.

**Category H: Sensory data. [Collected: No]**

Examples: Audio, electronic, visual, thermal, olfactory, or similar information.

**Category I: Professional or employment-related information. [Collected: No]**

Examples: Current or past job history or performance evaluations.

**Category J: Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)). [Collected: No]**

Examples: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.

**Category K: Inferences drawn from other personal information. [Collected: No]**

Examples: Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

12.2 Public Information. Under CCPA, personal information does not include: publicly available information from government records, de-identified or aggregated consumer information, and information excluded from the CCPA's scope such as; health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data, or Personal Information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994

12.3 Sources of Personal Information. The Provider may obtain the categories of personal information listed above from the following categories of sources:

**Directly from Authorized User:** Examples: From the forms Authorized User complete on our Service, preferences.

**Indirectly from Authorized User:** Examples: From observing Authorized User activity on our Service.

**Automatically from Authorized User:** Examples: Through Service-related Cookies set on Devices as the Authorized User navigates the Service.

**From Service Providers:** Examples: Other third-party vendors that Provider uses to provide the Service to Authorized User.

12.4 Use of Personal Data for Business Purposes or Commercial Purposes. The Provider may use or disclose Personal Data collected for business purposes or commercial purposes (as defined under the CCPA), which may include the following examples: to operate the Service, provide Authorized User with the Service, to provide Authorized User with support and to respond to inquiries, to investigate and address Authorized User concerns, and monitor and improve the Service. The Provider may use or disclose Personal Data to fulfill or meet the reason the Authorized User provided the information, for example, contact information to ask a question about our Service.

12.5 Law Enforcement Disclosure. Requests by law enforcement and as required by applicable law, court order, or governmental regulations, as described to Authorized User when collecting Personal Data or as otherwise set forth in the CCPA, for internal administrative and auditing purposes, and to detect security incidents and

protect against malicious, deceptive, fraudulent, or illegal activity, including, when necessary, to prosecute those responsible for such activities.

- 12.6 Disclosure of Personal Information for Business Purposes or Commercial Purposes. The Provider may use or disclose and may have used or disclosed in the last twelve (12) months the following categories of personal information for business or commercial purposes:

**Category A: Identifiers**

**Category F: Internet or Other similar network activity**

**Category G: Geolocation data**

Please note that the categories listed above are those defined in the CCPA. This does not mean that all examples of that category of Personal Data were in fact disclosed but reflects our good faith belief to the best of our knowledge that some of that information from the applicable category may be and may have been disclosed. When the Provider discloses Personal Data for a business purpose or a commercial purpose, a contract is executed that describes the purpose and requires the recipient to both keep that Personal Data confidential and not use it for any purpose except performing the contract.

- 12.7 Sale of Personal Data. As defined in the CCPA, "sell" and "sale" mean selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data by the business to a third party for valuable consideration. This means the Provider may have received benefit in return for sharing Personal Data, but not necessarily a monetary benefit.

The categories listed below are those defined in the CCPA. This does not mean that all examples of that category of Personal Data were in fact sold, but reflects our good faith belief based on best knowledge that some information from the applicable category may be or may have been shared for value in return within the last twelve (12) months, particularly:

**Category A: Identifiers**

**Category F: Internet or other similar network activity**

**Category G: Geolocation data**

- 12.8 Share of Personal Information. The Provider may share Personal Data identified in the above categories with the following categories of third parties: service providers, affiliates, business partners, and third-party vendors to whom Authorized User authorized disclosure of Personal Data in connection with the Services provided.
- 12.9 Rights under the CCPA. The CCPA provides California residents with specific rights regarding Personal Data. If Authorized User has the following rights if a resident of California:

**The Right to Notice:** Authorized User has the right to be notified which categories of Personal Data are being collected and the purposes of its use.

**The Right to Request:** Under CCPA, Authorized User has the right to request that Provider disclose information to Authorized User about collection, use, sale, disclosure for business purposes and share of Personal Data. Once Provider receives and confirms the request, Provider will disclose to Authorized User: the categories of Personal Data collected, the categories of sources for the Personal Data collected about Authorized User, the business or commercial purpose for collecting or selling that Personal Data, the categories of third-parties with whom Provider shares that Personal Data, and the specific pieces of Personal Data collected about Authorized User. If the Provider sold Authorized User Personal Data or disclosed for a business purpose the Provider will disclose to the Authorized User the categories of Personal Data categories sold, and the categories of Personal Data categories disclosed.

**The right to say no to the sale of Personal Data (opt-out):** Authorized User has the right to direct Provider to not sell Personal Data. To submit an opt-out request please contact us.

**The right to delete Personal Data:** Authorized User has the right to request the deletion of Personal Data, subject to certain exceptions. After receiving and confirming Authorized User request, Provider will delete the Authorized User Personal Data from our records, unless an exception applies. Provider may deny the deletion

request if retaining the information is necessary to: Complete the transaction for which Provider collected the Personal Data, provide a good or service that Authorized User requested, take actions reasonably anticipated within the context of our ongoing business relationship with Authorized User, or otherwise perform our contract with Authorized User; Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities; Debug products to identify and repair errors that impair existing intended functionality; Exercise free speech ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law; Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.); Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if Authorized User previously provided informed consent; Enable solely internal uses that are reasonably aligned with consumer expectations based on Authorized User relationship with Provider; Comply with a legal obligation; or Make other internal and lawful uses of that information that are compatible with the context in which Authorized User provided it.

**The right not to be discriminated against:** Authorized User has the right not to be discriminated against for exercising any of consumer's rights, including by: Denying goods or services to Authorized User; Charging different prices or rates for goods or services, including the use of discounts or other benefits or imposing penalties; Providing a different level or quality of goods or services to Authorized User; Suggesting that Authorized User will receive a different price or rate for goods or services or a different level or quality of goods or services.

- 12.10 Exercising CCPA Data Protection Rights. In order to exercise any Authorized User rights under the CCPA, and if Authorized User is a California resident, Authorized User can contact Provider at the email below (last paragraph of this section). Only Authorized User, or a person registered with the California Secretary of State to represent the Authorized User, may make a verifiable request related to Authorized User Personal Data. Authorized User request to Provider must: provide sufficient information that allows Provider to reasonably verify Authorized User is the person about whom Personal Data is being collected and properly understand, evaluate, and respond to it. Provider cannot respond to Authorized User request if Provider cannot: verify Authorized User identity or authority to make the request and confirm that the Personal Data relates to Authorized User. Provider will disclose and deliver the required information free of charge within 45 days of receiving Authorized User verifiable request. The time-period to provide the required information may be extended once by an additional 45 days when reasonably necessary and with prior notice. Any disclosures by the Provider will only cover the 12-month period preceding the verifiable request's receipt. For data portability requests, Provider will select a format to provide Authorized User Personal Data that is readily useable and should allow Authorized User to transmit the information from one entity to another entity without hindrance.
- 12.11 Do Not Sell My Personal Information. Authorized User have the right to opt-out of the sale of Authorized User personal information. Once Provider receive and confirm a verifiable consumer request from Authorized User, we will stop selling Authorized User personal information. To exercise opt-out rights, please contact us.
- 12.12 "Do Not Track" Policy (DNT). A concept promoted by US regulatory authorities, in particular the U.S. Federal Trade Commission (FTC), for the Internet industry to develop and implement a mechanism for allowing internet users to control the tracking of their online activities across websites. As Required by California Online Privacy Protection Act (CalOPPA), this Service does not respond to Do Not Track signals. However, some third-party websites do keep track of Authorized User browsing activities and can be checked in an Authorized User's web browser settings. The Authorized User can enable or disable DNT by visiting the preferences or settings page.
- 12.13 California Civil Rights. Under California Civil Code Section 1798 (California's Shine the Light law), California residents with an established business relationship with us can request information once a year about sharing their Personal Data with third parties for the third parties' direct marketing purposes. If more information is requested under the California Shine the Light law, and if Authorized user is a California resident, Authorized User can contact Provider using the contact information provided below.
- 12.14 California Privacy Rights for Minor Users. California Business and Professions Code section 22581 allow California residents under the age of 18 who are registered users of online sites, services, or applications to request and obtain removal of content or information they have publicly posted. To request removal of such

data, and if Authorized User is a California resident, Authorized User can contact Provider using the contact information provided below and include the email address associated with the user account. Be aware that Authorized User request does not guarantee complete or comprehensive removal of content or information posted online and that the law may not permit or require removal in certain circumstances.

### **13. CHANGES TO THIS PRIVACY POLICY**

This EULA and Privacy Policy may be revised from time to time and any changes will be reflected in a revised posting of the EULA. Provider will inform Authorized User via email and/or a prominent notice on the Service, prior to the change becoming effective and update the "Last updated" date at the top of this EULA.

EULA Authorized Users are advised to review this Privacy Policy periodically for any changes. Changes to this EULA and associated Privacy Policy are effective when they are posted on this page.