# OPIE SOFTWARE DATA PROCESSING AGREEMENT

**THIS DATA PROCESSING AGREEMENT ("DPA")** is entered into by and between: _____(**Customer Name)** a _____ **(State/Province)** corporation, with a principal place of business address located at_____ _____**(Customer Address)** ("**Controller**") and ***O&P Digital Technologies LLC*** ("**Processor**") with a principal place of business located at 3870 NW 83rd St., Gainesville, Florida 32606. (Collectively referred to as the "**Parties**" or individually as a "**Party**".)

1. **THE SUBJECT MATTER OF THE AGREEMENT**

1.1 **Agreement.** The Controller and the Processor have executed the Master Solution Agreement and/or OPIE Software Subscription Agreement ("**Contract**"). "**Services**" means all services and activities which are to be provided or undertaken pursuant to the Contract and those services as it concerns how data will be managed.

1.2 **Processor Appointment.** The Controller hereby appoints the Processor to process Personal Data, as specified below, on its behalf and the Processor hereby accepts such appointment. The Personal Data shall be processed under the terms and conditions set forth in this Agreement and the Contract. To the extent there is any conflict between the provisions of this Agreement and those of the Contract, this Agreement prevails.

2. **THE PURPOSE AND MANNER OF THE PROCESSING**

2.1 **Purpose.** The Personal Data is processed by the Processor for the purpose of performance of the Services under the Contract.

2.2 **Limited Data Access of Processor.** The Processor is obliged to process the Personal Data only upon explicit instruction of the Controller, in accordance with the provision of the Contract, this Agreement, applicable privacy laws and other documented instructions between the Controller and the Processor.

3. **TERM OF THE AGREEMENT**

3.1 **Term.** This Agreement takes effect upon signing of the Agreement by both parties. It shall remain in effect for the duration of services, (the "Initial Term",) commencing on the date executed by the last of the parties (the "Effective Date"). This Agreement shall automatically renew for an additional one (1) month term (each a "Renewal Term") unless terminated in accordance with this Agreement. The Initial Term and Renewal Term shall collectively be referred to as the "Term."

3.2 **Termination.** This Agreement shall be terminated in accordance with its terms or by applicable law.

3.3 **Data in Custody of Controller.** The Personal Data that the Controller transfers to the Processor shall remain within the custody and control of the Controller and as between the Controller and the Processor, the Controller shall be the owner of such Personal Data.

3.4 **Third-Parties Not Covered.** Notwithstanding the above, Controller acknowledges and agrees that if the Controller shares or authorizes any third party or related party to receive and view Personal Data directly in the application or via the use of any application integrations, the further processing by such third party or related party is not covered by this Data Processing Agreement.

4. **OBLIGATIONS OF THE PROCESSOR**

4.1 **Processor Compliance.** Comply with all applicable Data Protection Laws, as set forth herein, in the processing of Personal Data;

4.2 **Limited Data Access.** Only process Personal Data on behalf of and in accordance with the Controllers' lawful written instructions from time-to-time (including as set out in the DPA) or as required for Processor to provide, manage and facilitate the provision of the Services, but only where such instructions are consistent with the terms of the DPA and only in respect of

the subject matter, duration, nature and purpose of the Services, and the type of Personal Data and categories of data subject relevant to the Services;

4.3 **Data Processing Restrictions.** Not process Personal Data other than on the Controllers' documented instructions, except if needed by applicable legislation to which Processor is subject, in which case Processor shall inform Controller of such requirement before processing unless prohibited by law;

4.4 **Authorized Persons Only.** Ensure that only authorized persons process such Personal Data and that such persons are required to maintain the confidentiality of such Personal Data, and

4.5 **Controller Collaboration.** Upon the Controllers' request, and at Controllers' cost, Processor shall provide the Controller with reasonable cooperation and assistance needed to fulfil the Controllers' obligation (if any) under the data protection laws to carry out a data protection impact assessment or any other similar assessment related to the Controllers' use of the Services, to the extent the Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor.

5. **OBLIGATIONS OF THE CONTROLLER**

5.1 **Rights of Controller.** Where the Controller transfers or otherwise makes available Personal Data to Processor in relation to the Services, the Controller warrants and affirms:

5.1.1 Controller Right to Transfer. Controller has the necessary rights to transfer or make available such Personal Data to Processor (including that it has, or has procured, the necessary legal authority, permissions and/or consents for Processor to process the Personal Data to provide the Services);

5.1.2 Controller Instructions to Processor. Controllers' instructions to Processor follow (and will not cause Processor to be in breach of) the Data Protection Laws or any Data Localization Laws; and

5.1.3 Controller Notice to Data Subjects. The Controller has taken reasonable steps to ensure that any Data Subjects are aware of, understand, and have been notified of use and control of processing to be undertaken, including by supplying any notices required by applicable law or Regulatory Authority, or has otherwise followed applicable Data Protection and Localization Laws, also as set forth herein, and relevant to where its Patients are located. This is in relation to informing Data Subjects concerning the Processing of their Personal Data included in the Controller data.

5.1.4 Sole Control. The Controller shall have sole responsibility for the accuracy, quality, and use of the Personal Data of its patients and staff to comply with legal guidelines. The Controller acknowledges, warrants, and affirms that its use of the Services will not violate the rights of any Data Subject, including the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data to the extent applicable under any consumer privacy laws as set forth here or as may be disclosed or other similar regulatory requirements. To the extent that there is a violation of any privacy or other rights of a Data Subject, Controller agrees to indemnify, insure, and defend Processor against any claim a Data Subject may make against Processor.

5.2 **Personal Data Processing.** The duration of processing, the nature and the purpose of processing, the types of Personal Data and categories of Data Subjects processed under the DPA are further specified in Schedule 1 to the DPA.

6. **SECURITY MEASURES**

6.1 **Processor Security.** Considering the state of the art, the cost of implementation and the nature, scope, context, and purpose of processing, Processor shall implement the relevant technical and organizational measures to ensure a reasonable level of security.

6.2 **Processor Employee Training.** The Processor will provide its employees and other staff engaged in processing of personal data with relevant and reasonable instructions on how to process the Personal Data, especially including the obligations to keep the data and the

information about technical and the organizational security measures adopted for the protection of the Personal Data confidential.

6.3 **Confidentiality.** Processor's employees and contractors shall be contractually bound to maintain the confidence of Personal Data and other confidential information and comply with applicable policies, standards, or requirements in relation to the confidentiality of personal data, as set forth herein. Processor shall specify that failure to comply with those policies, standards, or requirements will subject the parties involved to investigation which may result in a disciplinary action up to and including termination of employment or engagement by the Processor. The Controller may ask the Processor for submission of the documented evidence of compliance with the foregoing.

7. **SUB-PROCESSING**

7.1 **Appointment of Sub-Processors.** Controller acknowledges and agrees that:

7.1.1 Data Processor Affiliates (DPA). Processor affiliates may be retained as Sub-Processors; and

7.1.2 Third-Party Sub-Processors. Processor and its affiliates may engage third-party Sub-Processors in connection with the provision of the Services. Processor or a Processor affiliate will enter into a written agreement with the Sub-Processor that requires data protection obligations not less protective than those in the DPA, to the extent applicable to the nature of the Services provided by such Sub-Processor. In case the Sub-Processor does not fulfil its data protection obligations under such a written agreement with Processor, Processor will remain liable to the Controller for the performance of the Sub-Processor's obligations under such agreement.

7.2 **List of Current Sub-Processors**. The Processor shall make available a list of Sub-Processors for the Services. A current list of the Processor's Sub-Processors shall be documented and maintained. Processor will update the list to reflect any addition, replacement, or other changes to Processor's Sub-Processors.

7.3 **Authorization**. Controllers' acceptance of the DPA shall be considered written authorization for Processor to engage the Sub-Processors as reflected on the list of current Sub-Processors as of the date of signing the DPA. Processor will provide notification of new Sub-Processor(s) before authorizing any new Sub-Processor(s) to process Personal Data in connection with the provision of the applicable Services.

8. **SECURITY BREACHES**

**8.1** **Notification:** Processor shall notify the Controller without undue delay upon Processor becoming aware of a breach affecting personal data, providing the Controller with sufficient information to allow the Controller to meet any obligations to report or inform Data Subjects of the Personal Data breach.

8.2 **Remediation:** Processor shall make reasonable efforts to identify the cause of such data incident and take those steps as Processor deems necessary and reasonable to remediate the cause of such data incident to the extent the remediation is within Processor's reasonable control.

9. **DELETION OR RETURN OF PERSONAL DATA**

9.1 **Deletion:** Processor shall return and delete Personal Data to the Controller upon written request from Controller within 30 days of termination of DPA and to the extent allowed by applicable law, remove Controller data within 6 months of termination of the DPA, unless deletion of Personal Data is not technically possible using all reasonable efforts.

10. **AUDIT RIGHTS**

10.1 **Accountability:** Subject to reasonable access arrangements being agreed between the parties and except for disclosure of information which is confidential and/or privileged, Processor shall make available to the Controller, all relevant information necessary to prove compliance with

Processor's obligations under applicable law and allow for and contribute to audits conducted by the Controller or another auditor mandated by the Controller at the Controllers' cost.

10.2 **Legality of instructions:** Processor shall at once inform Controller if any Controller instructions related to processing of data as related to the provision of services appears to, in its opinion, to infringe on data protection laws.

11. **LEGALLY REQUIRED CHANGES:**

11.1 **Regulator changes:** Processor and Controller acknowledge that laws relating to privacy and data protection are evolving and that amendments to the DPA may be necessary to ensure compliance with such developments. The parties agree to take such action to address changes to the standards and requirements of any data protection and localization laws as applicable to one or both of the parties including negotiating in good faith to amend the DPA as necessary or prudent for compliance with such laws.

12. **DATA PROCESSING TERMS (CANADA SPECIFIC PROVISIONS)**

12.1 **Scope of This Section.** Sections 12.1 to 12.8 shall apply only with respect to the processing of Personal Information (as defined in the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")) of Canadian Data Subjects on behalf of Controller operating within Canada. For greater clarity, the obligations regarding Personal Data set forth in Sections 1 through 11 and 16 through 35** of this Agreement shall continue to apply to the Personal Information of Canadian Data Subjects, except to the extent they are modified by Sections 12.1 to 12.8. Any questions that Controller or its customers have as it concerns Canadian provincial data privacy law should be directed to compliance@opiesoftware.com.

12.2 **Compliance with Canadian Privacy Laws:** Processor will process Personal Information in accordance with the requirements of PIPEDA.

12.3 **Protection of Personal Data:** Processor will use appropriate measures to protect Personal Information against loss, theft, and unauthorized access, use, disclosure, copying, destruction, or modification.

12.4 **Consent requirements:** Controller shall supply all required notices and obtain all required consents necessary for Processor to access, use, store and otherwise process Personal Information, including outside of Canada. Controller hereby agrees to indemnify and hold harmless, the Processor and its affiliates and Sub-Processors from any and all sanctions imposed for failure to comply with the consent requirements enabling Processor to process Personal Information. Processor will take reasonable steps to ensure that Personal Information transferred outside the province where such information is collected is not used for any unauthorized purpose and that Personal Information accessed, used, stored, or otherwise processed outside Canada is protected by reasonable safeguards.

12.5 **Controller Record Keeping:** Controller shall keep appropriate records and all consents obtained, and Controller shall promptly supply evidence of such consents to Processor upon request.

12.6 **Data minimization:** Controller shall provide Processor with only the minimum Personal Information required by Processor to supply the services.

12.7 **Cooperation:** The parties agree to reasonably cooperate and assist each other to comply with their respective obligations under PIPEDA, including to the extent permitted by applicable laws to respond to audits, requests, demands and investigations by any regulatory authority.

12.8 **Roles and Responsibilities of the Parties**: Processor will process Personal Information as a service provider and strictly for the purposes of performing the contracted services or as required by applicable laws.

Quality of Personal Information: Controller shall take reasonable steps to ensure the Personal Information it provides to Processor is accurate, up to date and complete, and relevant, having regard to Processor's use of the Personal Information.

Access to and corrections of Personal Information: If Processor receives an inquiry from a Canadian Data Subject relating to the Data Subject's right to access, modify or correct their Personal Information, Processor shall notify Controller and shall provide Controller with information reasonably required by Controller in respect of the request.

Breach Notification. In the event of a breach of security safeguards (as defined in PIPEDA) in respect of Personal Information, or a breach of the requirements of this Agreement, Processor shall advise Controller as soon as reasonably practicable upon becoming aware of the breach and shall comply with the requirements of Sections 8.1 and 8.2.

**13. DATA PROCESSING TERMS (AUSTRALIA SPECIFIC PROVISIONS)**

**13.1 Personal Information processed by an "APP Entity" (Australia)**

13.2 **Defined terms in this Section.** "APP Entity" has the meaning as set out in section 6(1) of the Australian Privacy Act. "Australian Privacy Act" means the *Privacy Act 1988* (Cth) as amended from time to time. "Australian Privacy Principle" (APP) has the meaning given by section 14 of the Australian Privacy Act. "Personal Information" has the meaning as set out in section 6(1) of the Australian Privacy Act. "Personal Health Data" has the meaning as set out in section 6FA of the Privacy Act. "Privacy Legislation" means such laws as may place requirements on the handling of Personal Information under the Australian Privacy Act and the Australian Privacy Principles. "Sensitive Information" has the meaning as set out in section 6(1) of the Australian Privacy Act.

13.3 **Scope of this Section.** Sections 12.1 to 12.8 shall apply only with respect to processing of Personal Information by recognized APP Entities operating within Australia or one of its external territories. For the purposes of this document, the Controller and the APP Entity are one and the same. The terms "Personal Information" and "Personal Data" shall be construed as the same for the purposes of this document.

13.4 **Compliance with the Australian Privacy Act:** Controller will process the Personal Information in accordance with all applicable provisions of the Australian Privacy Act and Privacy Legislation.

13.5 **Protection of Personal Information:** Processor will take reasonable steps to protect Personal Data against unauthorized access, use, disclosure, destruction, or alteration in accordance with its obligations under the Australian Privacy Act and Privacy Legislation.

13.6 **Consent requirements:** Controller shall obtain all required consents necessary for Processor to access, use, store and otherwise process Personal Information and/or Sensitive Information outside of Australia or an Australian external Territory. Controller hereby agrees to indemnify and hold harmless, the Processor and its affiliates and Sub-Processors from any and all sanctions imposed for failure to comply with the consent requirements enabling Processor to process Personal Health Data, as well as any breach of the Australian Privacy Principles. Processor will take reasonable steps to ensure that Personal Data transferred outside the province where such information is collected is not used for any unauthorized purpose and that Personal Data accessed, used, stored, or otherwise processed outside of Australia or an Australian external Territory is protected by reasonable safeguards.

13.7 **Controller Record Keeping:** Controller shall keep appropriate records of all consents obtained, and Controller shall promptly supply evidence of such consents to Processor upon request.

13.8 **Data minimization:** Controller shall ensure that the Controller data has only the minimum personal data required by Processor to supply the services.

13.9 **Cooperation:** The parties agree to reasonably cooperate and assist each other to comply with their respective obligations under the Australian Privacy Act and Privacy Legislation, including the extent permitted by applicable laws to respond to audits, requests, demands and investigations by any regulatory authority.

13.10 **Roles and Responsibilities of the Parties:** Processor will process personal data as a service provider strictly for the purposes of performing the contracted services or as required by applicable laws.

13.10.1 Anonymity and Pseudonymity: Processor, upon request, shall give individuals the option of not identifying themselves, or of using a pseudonym unless a limited exception applies.

13.10.2 Collection of solicited Personal Information: Processor will only collect Personal Information and will ensure that the higher standards are applied to the collection of Sensitive Information. Any unsolicited Personal Information, shall be dealt with in accordance with the APP.

13.10.3 Direct marketing: An organisation may only use or disclose Personal Information for direct marketing purposes if certain conditions are met.

13.10.4 Cross-border disclosure of Personal Information: Upon request, Processor shall provide information on the steps an APP Entity must take to protect Personal Information before it is disclosed overseas.

13.10.5 Adoption, use or disclosure of government related identifiers: Upon request, Processor shall outline the limited circumstances when it, if at all, may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

13.10.6 Quality of Personal Information: Processor shall take reasonable steps to ensure the Personal Information it collects is accurate, up to date and complete, and relevant, having regard to the purpose of the use or disclosure.

13.10.7 Security of Personal Information: Processor shall take reasonable steps to protect Personal Information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify Personal Information in certain circumstances.

13.10.8 Access to Personal Information: Upon request, Processor shall outline the limited circumstances when an individual shall be given access to Personal Information held about them by the entity. Processor acknowledges that it shall provide this access, unless a specific exception applies. Parties acknowledge that the Privacy Act 1988 contains exemptions to the disclosure of information. As such, personal and sensitive information may be disclosed where compelled by law, or where requested by the individual whom the information relates to. Based upon the relationship between the Controller and Processor, the Parties acknowledge that the Controller may need to request access or copies of the information to produce where compelled by law.

13.10.9 Correction of Personal Information. Upon request, Processor shall correct the Personal Information it holds about individuals if incorrect.

13.10.10 In the Event of a Breach. Parties acknowledge that the Privacy Act has strict obligations for APP entities to adhere to in the event of a data breach. This includes, yet is not limited to notifying the Australian Information Commissioner to follow the process in relation to Australia's mandatory notice of breach regime. In the event of a breach, Controller shall be responsible for notifying the Australian Information Commissioner, and also expressly set out that in the event of any loss, or unauthorised access or disclosure of Personal Data or Personal Health Data, the Processor must notify the Controller within 15 days.

14. **DATA PROCESSING TERMS (SAUDI ARABIA SPECIFIC PROVISIONS)**

14.1 **Scope of Data Processing Terms.** Section 14.1 to 14.8 shall apply only with respect to processing of Personal Data about Data Subjects in Saudi Arabia on behalf of Controller operating within Saudi Arabia.

14.2 **Compliance with Saudi Arabian Privacy Laws:** Controller will comply with applicable provisions of the Personal Data Protection Law, implemented by Royal Decree M/19 of 17 September 2021, including revisions or replacement documents.

14.3 **Protection of Personal Data:** Processor will take reasonable steps to protect Personal Data against unauthorized access, use, disclosure, destruction, or alteration.

14.4 **Consent requirements:** Controller shall supply all required notices and obtain all required consents necessary for Processor to access, use, store and otherwise process Personal Data

and/or Personal Health Data outside of Saudi Arabia. Controller hereby agrees to indemnify and hold harmless, the Processor and its affiliates and Sub-Processors from any and all sanctions imposed for failure to comply with the consent requirements enabling Processor to process Personal Health Data. Processor will take reasonable steps to ensure that Personal Data transferred outside the country where such information is collected is not used for any unauthorized purpose and that Personal Data accessed, used, stored, or otherwise processed outside Saudi Arabia is protected by reasonable safeguards.

14.5 **Controller Record Keeping:** Controller shall keep appropriate records of all notices supplied and all consents obtained, and Controller shall promptly supply evidence of such notices and consents to Processor upon request.

14.6 **Data minimization:** Controller shall ensure that the Controller data has only the minimum Personal Data required by Processor to supply the services.

14.7 **Cooperation:** The parties agree to reasonably cooperate and assist each other to comply with their respective obligations under the Royal Personal Data Protection Law, including the extent permitted by applicable laws to respond to audits, requests, demands and investigations by any regulatory authority.

14.8 **Roles and Responsibilities of the Parties:** Processor will process personal data as a service provider strictly for the purposes of performing the contracted services or as required by applicable laws.

15. **CALIFORNIA RESIDENTS.**

15.1 **CCPA Compliance.** If you are a California resident or have customers that are, then yours and our privacy practices comply with the California consumer privacy act of 2018 ("CCPA") cal. Civ. Code § 1798, and any CCPA-specific information is identified in this policy. The CCPA affords California consumers the right to obtain from us Personal Information about you that we collect, use, and disclose. To submit a request to know about the Personal Information we collect about you, please contact us at to compliance@opiesoftware.Com. O&P Digital Technologies LLC provides California citizens the following rights under the CCPA.

15.2 **Right to know**. This allows you to request information about what Personal Information is collected, used, shared or sold.

15.3 **Right to delete**. This allows you to request that we delete any Personal Information about you which we collect from you.

15.4 **Right to opt-out**. This allows you, if any sales were to occur, to request that we stop selling your Personal Information to third parties.

15.5 **Right to non-discrimination**. This affords you protection against any discrimination from us because of your decision to exercise your CCPA rights. If you choose to exercise your privacy rights, you have the right to not receive discriminatory treatment or a lesser degree of service from us.

15.6 **We Do Not Sell Your Personal Information**. O&P Digital Technologies LLC websites will never sell your Personal Information. However, California law requires that we maintain a separate webpage that allows you to opt out of the sale of your Personal Information. This link is available at https://www.opiesoftware.com/opt-out.

15.7 **Types of Personal Data**. The following are categories of Personal Data defined under the Act that we may receive in the course of administering the Services: Identifiers, Personal Information as described in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), Protected classification characteristics under California or federal law, Commercial information, Biometric information, Internet or other electronic network activity, Geolocation data, Sensory data, Professional or employment-related information, Non-public education information, and inferences drawn from other Personal Information.

15.8 **Exercising these rights.** To exercise any of these rights, please email Compliance@opiesoftware.com. with SUBJECT: PERSONAL DATA REQUEST.

15.9 **Mechanism for redress.** Any complaints, abuse, or concerns with regard to the use, processing, and disclosure of Personal Data provided by you or breach of these terms should immediately be communicated in writing or through email to Compliance@opiesoftware.com. We may reach out to you to confirm or discuss certain details about your complaint and issues raised. We are not responsible for any communication, if addressed, to any non-designated person in this regard.

15.10 **Requested Information.** We request you to please provide the following information in your complaint:

15.10.1 Identification of the information provided by you;

15.10.2 Clear statement as to whether the information is personal data or sensitive Personal Information;

15.10.3 Your address, telephone number or email address;

15.10.4 A statement that you have a good-faith belief that the personal data has been processed incorrectly or disclosed without authorization, as the case may be;

15.10.5 A statement, under penalty of perjury, that the information in the notice is accurate, and that the information being complained about belongs to you;

15.11 **Protecting Your Personal Data.** Protection from Unauthorized Access to or Alteration, Disclosure, or Destruction of Data. We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. This includes internal reviews of our data collection, storage and processing practices, and security measures, including appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal data.

15.12 **Limitations to Protection.** However, as effective as our security measures are, no security system is perfect. We cannot guarantee the security of our database, nor can we guarantee that the information you supply will not be intercepted while being transmitted to us over the Internet.

15.13 **Limitations to Liability.** We assume no liability or responsibility for disclosure of your information due to errors in transmission, unauthorized third-party access, or other causes beyond our control.

16. **NOTIFICATION IF PRIVACY POLICY CHANGES**

16.1 **Policy Changes.** As we improve our services in the future, we may need to change this privacy policy. If this policy changes, we will alert you to such changes by placing a notice on our webpage, our mobile application, and/or by some other means. If you use the services after any changes to the privacy policy have been posted, you are agreeing to all of the changes.

16.2 **How to Withdraw Consent; Mechanism to Withdraw Consent:**

16.2.1 **Requesting Deletion of User Information.** You can request the company delete your information. In some cases, however, we may retain information for a limited period for legitimate business or legal purposes.

16.2.2 **Who to Contact to Delete Personal Data?** To delete your personal data, please share your request to compliance@opiesoftware.Com with the subject “PERSONAL DATA REQUEST / DELETION REQUESTED”.

16.2.3 **Request Processing Time.** Please note that there may be delays between your request and deletion of the data, as we try to ensure protection of your information against accidental or malicious deletion requests.

16.3 **European Economic Area Residents**. If you are a resident of the European economic area (EEA) or European union (EU), this privacy policy also complies with the additional rights and protections afforded to residents of the European union as required by the general data privacy regulation (“GDPR”). Regulation 2016/679, general data protection regulation, 2016 O.J. (L 119). To exercise any of the rights and protections stated under this provision, please contact us at to compliance@opiesoftware.com.

16.3.1 **Data Transfers.** When we provide services, we are collecting and processing data that may contain personally identifiable information. This personally identifiable information is collected and processed via encrypted (or secure) servers.

16.3.2 **Data Transferred to Other Countries.** Our services are always conducted in a secure environment. We may transfer to and store the Personal Information we collect in countries other than the country in which the data was originally collected. Those countries may not have the same data protection as the country in which you provided the data. When we transfer your data to other countries, we will protect the data as described in this privacy policy and comply with applicable legal requirements providing adequate protection for the transfer of data to countries outside the European union (EU).

16.3.3 **Privacy Rights Under the GDPR.** Citizens of the EU and UK have the following rights that O&P Digital Technologies LLC acknowledges and will safeguard below.

16.3.3.1 **Right to be Informed.** You have the right to be informed about the collection and use of your Personal Information.

16.3.3.2 **Right of Access.** This allows you to receive a copy of your data and to check how your data is being processed.

16.3.3.3 **Right of Rectification.** This allows you to correct any incomplete or inaccurate information about you within our system.

16.3.3.4 **Right to Erasure (also known as right to be forgotten).** This allows you to request we delete or remove your personal data, under certain conditions.

16.3.3.5 **Right to Restrict Processing.** This allows you to request that we restrict the processing of your data, under certain conditions.

16.3.3.6 **Right to Object to Processing.** This allows you to object to processing of Personal Information in certain circumstances. It includes the right to stop the use of Personal Information for direct marketing.

16.3.3.7 **Data Portability.** This allows you to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.

16.3.3.8 **Right to Human Intervention.** Right to request not to be subject to automated decision making. This allows you to request the intervention of a human.

## 17. DECLARATION OF THE CONTROLLER

17.1 The Controller hereby warrants and represents that it seeks and will obtain professional, technological, organizational, and personal skills and competence to ensure security of processing of Personal Data by the Processor.

17.2 The Controller shall provide the Processor with all assistance and cooperation necessary for fulfilment of purpose of this Agreement, protection of Personal Data from any abuse or breach and for compliance with relevant legislation when processing the Personal Data.

17.3 If any proceeding is opened by the competent data protection authority or court in connection with the processing of Personal Data upon a motion from a data subject, the Parties undertake to provide each other with all necessary assistance in these proceedings upon request.

## 18. CONFIDENTIALITY OF THE INFORMATION

Except as provided below, each party acknowledges that all information furnished or disclosed by the other party that is marked “confidential,” “proprietary,” or with a similar legend, or if not so marked, is identified as confidential at time of disclosure and confirmed in writing within ten (10) days thereafter, and (whether or not marked confidential) all Software, business plans, new product information, technical information, and sales is “Confidential Information” of the disclosing party. The receiving party agrees that it will not permit the duplication, use, or disclosure of any such Confidential Information to any third party (other than employees, agents, or contractors of it or its affiliates who agree in writing to maintain the confidentiality of the Confidential Information in accordance with the terms of this Agreement). The receiving party shall take appropriate action, by instruction, agreement, or otherwise, with any person

permitted access to the Confidential Information so as to enable it to satisfy its obligations hereunder. "Confidential Information" shall not include any information which (i) at the time of disclosure is in the public domain; (ii) after disclosure is published or otherwise becomes part of the public domain through no fault of the receiving party; or (iii) the receiving party can document already was in its possession at the time of disclosure hereunder or which rightfully comes into its possession from a third-party source.

19. **MUTUAL NON-SOLICITATION.** Neither party shall, during the Term, and for one (1) year thereafter, directly or indirectly hire or attempt to hire any employee of the other party who performed work on any project covered by this Agreement without such other party's prior written consent; provided that the foregoing shall not prohibit either party from issuing advertisements of a general nature not specifically directed at any such employee and hiring any such employee so long as such party is in compliance with this Section 19.

20. **MUTUAL NON-COMPETITION.** During, and for one (1) year after termination of this agreement, the Processor and the Controller agree not to: (i) divert, take away or solicit any of each parties' actual or potential customers that have been introduced or made known to either party by the other party or (ii) solicit, employ or attempt to employ, any of either parties' personnel, vendors, and/or contractors or (iii) compete with the other party's business. The term "not compete" as used herein shall mean that either party shall not own, manage, or operate a business substantially similar to or competitive with the present business of either party.

21. **GOVERNING LAW.** This agreement shall be governed in substance exclusively by the internal laws of the state of Florida and procedurally through the rules of the American Arbitration Association, without regard to its conflicts of laws rules. The State and federal courts located in the state of Florida shall have exclusive jurisdiction to enforce any decision from an arbitrator of the parties. Each party hereby consents to the exclusive jurisdiction of such courts to enforce the decision of the arbitrator. The United Nations convention on contracts for the international sale of goods is hereby excluded in its entirety from application of this agreement**.**

22. **ATTORNEY'S FEES.** The prevailing party in disputes concerning this agreement shall be entitled to recover its costs for enforcement, including but not limited to reasonable attorney's fees, arbitration costs and court costs and all necessary expenses. Notwithstanding anything in this agreement to the contrary, in the event of customer's bankruptcy or insolvency, OPIE will be entitled to recover from customer its costs and expenses, including, without limitation, reasonable attorneys' fees and costs, that OPIE incurs enforcing and/or otherwise protecting its rights and remedies under this agreement or amendments and modifications thereto.

23. **AMBIGUITY.** Each party and its counsel have participated fully in the review and revision of this agreement. Any rule of construction to the effect that ambiguities are to be resolved against the drafting party shall not apply in interpreting this agreement.

24. **ENTIRE AGREEMENT.** Except as provided herein, this agreement is the entire agreement between the parties, and all prior negotiations, representations, or agreements between the parties are merged into this agreement.

25. **SEVERABILITY.** The invalidity, in whole or in part, of any provision of this agreement shall not affect the validity or enforceability of any other of its provisions.

26. **HEADINGS.** The paragraph or section headings in this agreement are used for convenience

only. They form no part of this agreement and are in no way intended to alter or affect the meaning of this agreement.

27. **APPLICABLE LAW; PERSONAL JURISDICTION; VENUE.** This agreement shall be construed in accordance with and all disputes hereunder shall be governed by the laws of the state of Florida. All parties to this agreement agree to submit to personal jurisdiction in the state of Florida. Any dispute that arises under or relates to this agreement (whether contract, tort, or both) shall be resolved through the Dispute Resolution clause in binding arbitration and enforced in the applicable federal or state court in the state of Florida.

28. **INDEMNIFICATION.** Controller agrees to indemnify, defend and forever hold Processor (and its parents, affiliates, subsidiaries or entities under common ownership or control) and all of its respective present and former officers, members, shareholders, directors, employees, representatives, attorneys, insurers and agents, and their successors, heirs and assigns (each, in such capacity, an "indemnified party" and, collectively, the "indemnified parties"), harmless from and against any and all third-party losses, liabilities, claims, costs, damages and expenses (including, without limitation, fines, forfeitures, outside attorneys' fees, disbursements and administrative or court costs) arising directly or indirectly out of or relating to (1) a breach by Controller of this agreement or of any representation, warranty, covenant or agreement contained herein (2) intentional, wilful, wanton, reckless or negligent conduct on the part of Controller (3) any content on the site ("content" includes but is not limited to domain name, marketing and advertising content, but excludes content provided by Processor or required by Processor to be on the site), which results in any claim of trademark or copyright infringement, libel, defamation, breach of confidentiality, false or deceptive advertising or sales practices, deceptive use of URL names, cybersquatting/domain name issues, consumer fraud, injury, damage or harm of any kind to any person or entity or (4) a claim of breach of data security by a customer. Should any of the above-named claims be brought against Processor (i) Processor shall promptly notify Controller of any matters in respect to which the indemnity may apply and of which Processor has knowledge; (ii) give Controller the right to control the defense and all negotiations relative to the settlement of any such claim; and (iii) shall cooperate with Controller, at Controller's cost and expense in the defense or settlement thereof. Should Processor choose to participate in such defense and in any settlement discussions directly or through counsel of its choice on a monitoring, non-controlling basis, Processor's costs shall be borne by Controller. Furthermore, Processor shall have the right to take over the defense, and Processor's costs shall be borne by Processor.

29. **LIMITATION OF LIABILITY.** Processor does not make, and hereby expressly waives, any warranties express or implied. PROCESSOR SHALL HAVE no LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE FOR CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, OR PUNITIVE DAMAGES EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

30. **PROOF OF INSURANCE.** Upon request, Controller shall provide Processor with certificates evidencing the existence of the following insurance coverage: (A) comprehensive general liability (including contractual and completed operations coverage) of $1,000,000.00 combined single limit; (B) umbrella liability coverage in an amount not less than $1,000,000.00; and (C) cyber liability and "errors and omissions" insurance or professional liability or malpractice insurance in an amount not less than $1,000,000.00. Nothing herein shall be construed as a limitation of Controller liability. Failure to provide and maintain the insurance required by this agreement will constitute a material breach of the agreement.

31. **FORCE MAJEURE.** If the performance of this agreement, or any obligation hereunder is

prevented, restricted or interfered with by any act or condition whatsoever beyond the reasonable control of the affected party including but not limited to acts of god, labor disputes, pandemic, extreme weather or delays or interruptions to services provided by cloud, platform, or other software as a service providers which may impact the O&P services(including but, not limited to amazon webservices), the party so affected, upon giving prompt notice to the other party, shall be excused from such performance to the extent of such prevention, restriction or interference. Notwithstanding the foregoing, payment obligations owed under this agreement shall not be excused due to any such act or condition.

32. **COUNTERPARTS.** This agreement may be executed in two or more counterparts, each of which shall be an original, but all of which shall constitute one and the same instrument.

33. **BINDING EFFECT.** This agreement shall bind and inure to the benefit of the heirs, personal representatives, successors, and permitted assigns of the parties.

34. **MODIFICATIONS.** No supplement, modification, or amendment to this agreement will be binding unless executed in writing by both parties.

35. **WAIVER.** Any term or provision of this agreement may be waived in writing at any time by the party entitled to the benefit thereof. No waiver of any of the provisions of this agreement will be deemed or will constitute a waiver of any other provision, whether or not similar, nor will any waiver constitute a continuing waiver.

36. **ASSIGNMENT.** Either party to this agreement may assign any of its rights or delegate any of its duties under the agreement without the prior written consent of the other party.

| **CUSTOMER** "**Controller**" | **O&P Digital Technologies LLC** "**Processor"** |
|---|---|
| By: Authorized Signature | By: Authorized Signature |
| Printed Name | Printed Name |
| Title | Title |
| Date | Date |

## OPIE SOFTWARE DATA PROCESSING AGREEMENT

### Schedule 1

**TECHNICAL AND ORGANIZATIONAL MEASURES FOR SECURITY OF PROTECTION OF PERSONAL DATA**

1. **Statutory obligations of the Processor**

1.1 The Processor is obliged:

(a) to prevent any unauthorized persons to access to Personal Data and means for their processing;

(b) to prevent any unauthorized reading, creating, copying, transferring, modifying, or deleting of records containing Personal Data; and

(c) to adopt measures to identify and verify to whom the Personal Data were transferred.

(d) adopt policies setting forth the rules for accessing and further processing the Personal Data.

1.2 In the area of automatic processing of Personal Data, the Processor is also obliged:

(a) to ensure that the systems for automatic processing of Personal Data are used only by authorized persons;

(b) to ensure that the natural persons authorized to use systems for automatic processing of Personal Data have access only to the Personal Data corresponding to their authorization and on the basis of specific user authorizations established exclusively for these persons;

(c) to make electronic records identifying and verifying when, by whom and for what reason the Personal Data were recorded or otherwise processed; and

(d) to prevent any unauthorized access to data carriers.

1.3 **Physical Access**

The Processor maintains physical security standards designed to prohibit unauthorized physical access to Processor facilities and equipment. This is accomplished by the following practices:

- physical access to locations is limited to Processor's employees, subcontractors, and authorized visitors;
- Processor's employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises;
- monitoring access to Processor's facilities, including restricted areas and equipment within facilities;
- maintaining an audit trail of access.

1.4 **Access Control and Administration**

The Processor maintains the following standards for access control and administration of the relevant IT environment.

- administrator accounts are only be used for the purpose of performing administrative activities;
- each account with administrative privileges is traceable to a uniquely identifiable individual;
- all access to computers and servers is be authenticated and within the scope of an employee's job function;
- the display and printing of passwords is masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them;
- passwords must be uniquely identifiable to an individual;
- passwords must be encrypted when transmitted;

- password complexity should never be less than 3 out of 4-character classes and must have character class choices such as upper-case letters, lower case letters, numeric digits, or special characters;
- automatic time-out of access to computers and servers if left idle with the requirement for password authentication for re-access;
- accounts must be set to lockout after several erroneous failed login attempts.

1.5 **Virus Scanning and Logging**

Computers and servers have reasonable up-to-date versions of system security agent software which may include host firewall, anti-virus protection and up-to-date patches and virus definitions. Such software is configured to scan for and promptly remove or fix identified findings.

The Processor maintains logs of various components of the infrastructure and an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other actual and threatened security risks.

1.6 **Processor's Personnel**

Employees and contractors are trained on the Processor's privacy and security policies and made aware of their responsibilities regarding privacy and security practices.

The Processor's employees and contractors are contractually bound to maintain the confidence of Controller's Personal Data or confidential information and comply with applicable Processor's policies, standards, or requirements in relation to the processing of Controller's Personal Data. Failure to comply with those policies, standards or requirements will be subject to investigation which may result in disciplinary action up to and including termination of employment or engagement by the Processor.

The Processor's employees and contractors shall have access to Personal Data only on need-to-know basis in compliance with access rules stated in clause 2.1 and 2.2 above.

1.7 **Security Breach Notification and Security Incident Management**

In the event the Processor confirms a security breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed ("**Security Incident**"), the Processor will without undue delay notify the Controller of the Security Incident. The Processor will provide the Controller with updates on the status of the Security Incident until the matter has been remediated. The reports will include, without limitation, a description of the Security Incident, actions taken and remediation plans.

Notice of a Security Incident shall be provided to the Controller via email address to:

_____

**[Controller Emergency Response Email]**

Similarly, if the Controller becomes aware of a Security Incident that affects the Services, the Controller shall promptly notify the Processor of such and inform the Processor of the scope of the Security Incident. Notice shall be provided to the Processor via email address to emergencyresponse@opiesoftware.com.