Data Protection Addendum

This Data Protection Addendum (“Addendum”) forms part of the Terms of Service between Merchant and oneapp covering Merchant’s use of the SaaS (as defined below) (“Agreement”).

I. Introduction

1. Definitions

- “Applicable Data Protection Law” means all laws and regulations applicable to oneapp’s processing of personal data under the Agreement.
- “controller” means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- “Merchant Account Data” means personal data that relates to Merchant’s relationship with oneapp, including the names or contact information of individuals authorized by Merchant to access Merchant’s account, and billing information of individuals that Merchant has associated with its account. Merchant Account Data also includes any personal data oneapp may need to collect for the purpose of identity verification (including providing the Multi-Factor Authentication SaaS, as defined below), or as part of its legal obligation to retain Subscriber Records (as defined below).
- “Merchant Content” means (a) personal data exchanged as a result of using the SaaS (as defined below), such as text message bodies, voice and video media, images, email bodies, email recipients, sound, and, where applicable, details Merchant submits to the SaaS from its designated software applications and services and (b) data stored on Merchant’s behalf such as communication logs within the SaaS or marketing campaign data that Merchant has uploaded to the SaaS (as defined below).
- “Merchant Data” has the meaning given in the Agreement. Merchant Data includes Merchant Account Data, Merchant Usage Data, Merchant Content, and Sensitive Data, each as defined in this Addendum.
- “Merchant Usage Data” means data processed by oneapp for the purposes of transmitting or exchanging Merchant Content utilizing phone numbers either through the public switched telephone network or by way of other communication networks. Merchant Usage Data includes data used to identify the source and destination of a communication, such as (a) individual data subjects’ telephone numbers, data on the location of the device generated in the context of providing the SaaS, and the date, time, duration and the type of communication and (b) activity logs used to identify the source of Service requests, optimize and maintain performance of the SaaS, and investigate and prevent system abuse.
- “Multi-Factor Authentication SaaS” means the provision of a portion of the SaaS under which Merchant adds an additional factor for verification of Merchant’s end users’ identity in connection with such end users’ use of Merchant’s software applications or services.
- “personal data” means any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “processor” means the entity which processes personal data on behalf of the controller.
- “processing” (and “process”) means any operation or set of operations performed on personal data or on sets of personal data,

whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- “Security Incident” means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Merchant Data.
- “Sensitive Data” means (a) social security number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), financial information, banking account numbers or passwords; (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords, mother’s maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of “special categories of data” under GDPR (as defined below) or any other applicable law or regulation relating to privacy and data protection.
- “SaaS” means the products and services provided by oneapp or its affiliates, as applicable, that are (a) used by Merchant, including, without limitation, products and services that are on a trial basis or otherwise free of charge or (b) ordered by Merchant under an order form.
- "Subscriber Records” means Merchant Account Data containing proof of identification and proof of physical address necessary for oneapp to provide Merchant or Merchant’s end users with services in certain areas. When required by law or regulation, Subscriber Records are shared with local service providers, or local government authorities.
- “sub-processor” means (a) oneapp, when oneapp is processing Merchant Content and where Merchant is a processor of such Merchant Content or (b) any third-party processor engaged by oneapp to process Merchant Content in order to provide the SaaS to Merchant. For the avoidance of doubt, telecommunication providers are not sub-processors.
- “Third Party Request” means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.
- “oneapp Privacy Notice” means the privacy notice for the SaaS, the current version of which is available at https://legal.withoneapp.com/#privacy.

Any capitalized term not defined in this Section 1 will have the meaning provided in this Addendum or the Agreement.

II. Controller and Processor

2. Relationship

2.1 oneapp as a Processor. Merchant and oneapp agree that with regard to the processing of Merchant Content, Merchant may act either as a controller or processor and oneapp is a processor. oneapp will process Merchant Content in accordance with Merchant’s instructions as set forth in Section 5 (Merchant Instructions).

2.2 oneapp as a Controller of Merchant Account Data. Merchant and oneapp acknowledge that, with regard to the processing of Merchant Account Data, Merchant is a controller and oneapp is an independent controller, not a joint controller with Merchant. oneapp will process Merchant Account Data as a controller in order to (a) manage the relationship with Merchant; (b) carry out oneapp’s core business operations, such as accounting and filing taxes; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the SaaS; (d) perform identity verification; (e) comply with oneapp’s legal or regulatory obligation to retain Merchant Records; and (f) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the oneapp Privacy Notice.

2.3 oneapp as a Controller of Merchant Usage Data. The parties acknowledge that, with regard to the processing of Merchant Usage Data, Merchant may act either as a controller or processor and oneapp is an independent controller, not a joint controller with Merchant. oneapp will process Merchant Usage Data as a controller in order to carry out the necessary functions as a SaaS provider, such as: (a) oneapp’s accounting, tax, billing, audit, and compliance purposes; (b) to provide, optimize, and maintain the SaaS, platform and security; (c) to investigate fraud, spam, wrongful or unlawful use of the SaaS; (d) as required by applicable law or regulation; or (e) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the oneapp Privacy Notice.

3. Purpose Limitation. oneapp will process personal data in order to provide the SaaS in accordance with the Agreement. Schedule 1 (Details of Processing) of this Addendum further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and categories of data subjects.

4. Compliance. Merchant is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the SaaS and its own processing of personal data and (b) it has, and will continue to have, the right to transfer, or provide access to, personal data to oneapp for processing in accordance with the terms of the Agreement and this Addendum.

III. oneapp as a Processor – Processing Merchant Content

5. Merchant Instructions. Merchant appoints oneapp as a processor to process Merchant Content on behalf of, and in accordance with, Merchant’s instructions (a) as set forth in the Agreement, this Addendum, and as otherwise necessary to provide the SaaS to Merchant, and which includes investigating security incidents and preventing spam, fraudulent activity, and violations of the oneapp Acceptable Use Policy, the current version of which is available at https://legal.withoneapp.com/#aup, and detecting and preventing network exploits or abuse; (b) as necessary to comply with applicable law or regulation, including Applicable Data Protection Law; and (c) as otherwise agreed in writing between Merchant and oneapp (“Permitted Purposes”).

5.1 Lawfulness of Instructions. Merchant will ensure that its instructions comply with Applicable Data Protection Law. Merchant acknowledges that oneapp is neither responsible for determining which laws or regulations are applicable to Merchant’s business nor whether oneapp’s provision of the SaaS meets or will meet the requirements of such laws or regulations. Merchant will ensure that oneapp’s processing of Merchant Content, when done in accordance with Merchant’s instructions, will not cause oneapp to violate any applicable law or regulation, including Applicable Data Protection Law. oneapp will inform Merchant if it becomes aware, or reasonably believes, that Merchant’s instructions violate any applicable law or regulation, including Applicable Data Protection Law.

5.2 Additional Instructions. Additional instructions outside the scope of the Agreement or this Addendum will be agreed to in writing between Merchant and oneapp, including any additional fees that may be payable by Merchant to oneapp for carrying out such additional instructions.

6. Confidentiality

6.1 Responding to Third Party Requests. In the event any Third Party Request is made directly to oneapp in connection with oneapp’s processing of Merchant Content, oneapp will promptly inform Merchant and provide details of the same, to the extent legally permitted. oneapp will not respond to any Third Party Request without Merchant’s prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Merchant.

6.2 Confidentiality Obligations of oneapp Personnel. oneapp will ensure that any person it authorizes to process Merchant Content has agreed to protect personal data in accordance with oneapp's confidentiality obligations in the Agreement.

7. Sub-processors

7.1 Authorization for Onward Sub-processing. Merchant provides a general authorization for oneapp to engage onward sub-processors that is conditioned on the following requirements:

(a) oneapp will restrict the onward sub-processor’s access to Merchant Content only to what is strictly necessary to provide the SaaS, and oneapp will prohibit the sub-processor from processing the personal data for any other purpose;

(b) oneapp agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Merchant Content to the standard required by Applicable Data Protection Law, including the requirements set forth in Schedule 2 (Jurisdiction Specific Terms) of this Addendum; and

(c) oneapp will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its sub-processors.

7.2 Current Sub-processors and Notification of Sub-processor Changes. Merchant consents to oneapp engaging third party sub-processors to process Merchant Content within the SaaS for the Permitted Purposes provided that oneapp maintains an up-to-date list of its sub-processors at https://legal.withoneapp.com/#sub-processors. If Merchant subscribes to such notifications, oneapp will provide details of any change in sub-processors as soon as reasonably practicable. With respect to changes in infrastructure providers, oneapp will endeavor to give written notice sixty (60) days prior to any change, but in any event will give written notice no less than thirty (30) days prior to any such change. With respect to oneapp's other sub-processors, oneapp will endeavor to give written notice thirty (30) days prior to any change, but will give written notice no less than ten (10) days prior to any such change.

7.3 Objection Right for new Sub-processors. Merchant may object to oneapp's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, Merchant and oneapp agree to discuss commercially reasonable alternative solutions in good faith. If Merchant and oneapp cannot reach a resolution within ninety (90) days from the date of oneapp's receipt of Merchant's written objection, Merchant may discontinue the use of the affected SaaS by providing written notice to oneapp. Such discontinuation will be without prejudice to any fees incurred by Merchant prior to the discontinuation of the affected SaaS. If no objection has been raised prior to oneapp replacing or appointing a new sub-processor, oneapp will deem Merchant to have authorized the new sub-processor.

8. Data Subject Rights. oneapp provides Merchant with a number of self-service features via the SaaS, including the ability to delete, obtain a copy of, or restrict use of Merchant Content. Merchant may use such self-service features to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to Third Party Requests from data subjects via the SaaS at no additional cost. Upon Merchant's request, oneapp will provide reasonable additional and timely assistance to Merchant in complying with Merchant's data protection obligations with respect to data subject rights under Applicable Data Protection Law to the extent Merchant does not have the ability to resolve a Third Party Request from a data subject through self-service features made available via the SaaS.

9. Impact Assessments and Consultations. oneapp will provide reasonable cooperation to Merchant in connection with any data protection impact assessment (at Merchant's expense only if such reasonable cooperation will require oneapp to assign significant resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Law.

10. Return or Deletion of Merchant Content. oneapp will, in accordance with Section 3 (Duration of the Processing) of Schedule 1 (Details of Processing) of this Addendum, delete or return to Merchant any Merchant Content stored within the SaaS.

10.1 Extension of Addendum. Upon termination of the Agreement, oneapp may retain Merchant Content in storage for the time periods set forth in Schedule 1 (Details of Processing) of this Addendum, provided that oneapp will ensure that Merchant Content (a) is processed only as necessary for the Permitted Purposes and (b) remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

10.2 Retention Required by Law. Notwithstanding anything to the contrary in this Section 10, oneapp may retain Merchant Content, or any portion of it, if required by applicable law or regulation, including Applicable Data Protection Law, provided such Merchant Content remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

IV. Security and Audits

11. Security

11.1 Security Measures. oneapp has implemented and will maintain the technical and organizational security measures as set forth in the Agreement.

11.2 Determination of Security Requirements. Merchant acknowledges the SaaS include certain features and functionalities that Merchant may elect to use which impact the security of Merchant Data processed by Merchant's use of the SaaS, such as, but not limited to, encryption of voice recordings, availability of multi-factor authentication on Merchant's account, or optional Transport Layer Security (TLS) encryption. Merchant is responsible for reviewing the information oneapp makes available regarding its data security, including its audit reports, and making an independent determination as to whether the SaaS meet the Merchant's requirements and legal obligations, including its obligations under Applicable Data Protection Law. Merchant is further responsible for properly configuring the SaaS and using features and functionalities made available by oneapp to maintain appropriate security in light of the nature of Merchant Data processed as a result of Merchant's use of the SaaS.

11.3 Security Incident Notification. oneapp will provide notification of a Security Incident in the following manner:

(a) oneapp will, to the extent permitted by applicable law or regulation, notify Merchant without undue delay, but in no event later than seventy-two (72) hours after oneapp's discovery of a Security Incident impacting Merchant Data of which oneapp is a processor;

(b) oneapp will, to the extent permitted and required by applicable law or regulation, notify Merchant without undue delay of any Security Incident involving Merchant Data of which oneapp is a controller; and

(c) oneapp will notify Merchant of any Security Incident via email to the email address(es) designated by Merchant in Merchant's account.

oneapp will make reasonable efforts to identify a Security Incident, and to the extent a Security Incident is caused by oneapp's violation of this Addendum, remediate the cause of such Security Incident. oneapp will provide reasonable assistance to Merchant in the event that Merchant is required under Applicable Data Protection Law to notify a regulatory authority or any data subjects impacted by a Security Incident.

12. Audits. Merchant and oneapp acknowledge that Merchant must be able to assess oneapp's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as oneapp is acting as a processor on behalf of Merchant.

12.1 oneapp's Audit Program. oneapp uses external auditors to verify the adequacy of its security measures with respect to its processing of Merchant Content. Such audits are performed at least once annually at oneapp's expense by independent third-party security professionals at oneapp's selection and result in the generation of a confidential audit report ("Audit Report").

12.2 Merchant Audit. Upon Merchant's written request at reasonable intervals, and subject to reasonable confidentiality controls, oneapp will make available to Merchant a copy of oneapp's most recent Audit Report. Merchant agrees that any audit rights granted by Applicable Data Protection Law will be satisfied by these Audit Reports. To the extent that oneapp's provision of an Audit Report does not provide sufficient information or Merchant is required to respond to a regulatory authority audit, Merchant agrees to a mutually agreed-upon audit plan with oneapp that: (a) ensures the use of an independent third party; (b) provides written notice to oneapp in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Merchant at oneapp's then-current rates; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Merchant; and (g) obligates Merchant, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

13. Jurisdiction Specific Terms. To the extent oneapp processes personal data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 2 (Jurisdiction Specific Terms) of this Addendum, the terms specified in Schedule 2 with respect to the applicable jurisdiction(s) apply in addition to the terms of this Addendum.

V. Miscellaneous

15. Cooperation and Data Subject Rights. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable) or (b) any Third Party Request relating to the processing of Merchant Account Data or Merchant Usage Data conducted by the other party, such party will promptly inform such other party in writing. Merchant and oneapp agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Law.

16. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Schedule 2 (Jurisdiction Specific Terms) of this Addendum; (2) the terms of this Addendum outside of Schedule 2 (Jurisdiction Specific Terms); (3) the Agreement; and (4) the oneapp Privacy Notice. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, without limitation, the exclusions and limitations set forth in the Agreement.

17. Updates. oneapp may update the terms of this Addendum from time to time; provided, however, oneapp will provide at least thirty (30) days prior written notice to Merchant when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing SaaS. The then-current terms of this Addendum are available at https://legal.withoneapp.com/#data-protection-addendum.

Schedule 1

Details of Processing

1. Nature and Purpose of the Processing. oneapp will process personal data as necessary to provide the SaaS under the Agreement. oneapp does not sell Merchant’s personal data or Merchant end users’ personal data and does not share such end users’ information with third parties for compensation or for those third parties’ own business interests.

1.1 Merchant Content. oneapp will process Merchant Content as a processor in accordance with Merchant’s instructions as set forth in Section 5 (Merchant Instructions) of this Addendum.

1.2 Merchant Account Data. oneapp will process Merchant Account Data as a controller for the purposes set forth in Section 2.2 (oneapp as a Controller of Merchant Account Data) of this Addendum.

1.3 Merchant Usage Data. oneapp will process Merchant Usage Data as a controller for the purposes set forth in Section 2.3 (oneapp as a Controller of Merchant Usage Data) of this Addendum.

2. Processing Activities

2.1 Merchant Content. Personal data contained in Merchant Content will be subject to the following basic processing activities:

(a) the provision of programmable communication products and services, primarily offered in the form of application programming interfaces, to Merchant, including transmittal to or from Merchant’s software applications or; services and designated third parties as directed by Merchant, from or to the publicly-switched telephone network or by way of other communications networks. Storage of personal data on oneapp’s network;

(b) the provision of products and services which allow the transmission and delivery of email communications on behalf of Merchant to its recipients. oneapp will also provide Merchant with analytic reports regarding the email communications it sends on Merchant's behalf. Storage of personal data on oneapp’s network; and

(c) the provision of products and services which allows Merchant to integrate, manage and control its data relating to end users. Storage of personal data on oneapp’s network.

2.2 Merchant Account Data. Personal data contained in Merchant Account Data will be subject to the processing activities of providing the SaaS.

2.3 Merchant Usage Data. Personal data contained in Merchant Usage Data will be subject to the processing activities of providing the SaaS.

3. Duration of the Processing. The period for which personal data will be retained and the criteria used to determine that period is as follows:

3.1 Merchant Content.

SaaS. Prior to the termination of the Agreement, (x) oneapp will process stored Merchant Content for the Permitted Purposes until Merchant elects to delete such Merchant Content via the SaaS and (y) Merchant agrees that it is solely responsible for deleting Merchant Content via the SaaS. Upon termination of the Agreement, oneapp will (i) provide Merchant thirty (30) days after the termination effective date to obtain a copy of any stored Merchant Content via the SaaS; (ii) automatically delete any stored Merchant Content thirty (30) days after the termination effective date; and (iii) automatically delete any stored Merchant Content on oneapp's back-up systems sixty (60) days after the termination effective date. Any Merchant Content archived on oneapp's back-up systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law or regulation.

3.2 Merchant Account Data. oneapp will process Merchant Account Data as long as required (a) to provide the SaaS to Merchant; (b) for oneapp's legitimate business needs; or (c) by applicable law or regulation. Merchant Account Data will be stored in accordance with the oneapp Privacy Notice.

3.3 Merchant Usage Data. Upon termination of the Agreement, oneapp may retain, use, and disclose Merchant Usage Data for the purposes set forth in Section 1.3 (Merchant Usage Data) of this Schedule 1, subject to the confidentiality obligations set forth in the Agreement. oneapp will anonymize or delete Merchant Usage Data when oneapp no longer requires it for the purposes set forth in Section 1.3 (Merchant Usage Data) of this Schedule 1.

4. Categories of Data Subjects

4.1 Merchant Content. Merchant's end users.

4.2 Merchant Account Data. Merchant's employees and individuals authorized by Merchant to access Merchant's oneapp account or make use of the Multi-Factor Authentication SaaS received from oneapp.

4.3 Merchant Usage Data. Merchant's end users.

5. Categories of Personal Data. oneapp processes personal data contained in Merchant Account Data, Merchant Content, and Merchant Usage Data.

6. Sensitive Data or Special Categories of Data

6.1 Merchant Content. Sensitive Data may, from time to time, be processed via the SaaS where Merchant or its end users choose to include Sensitive Data within the communications that are transmitted using the SaaS. Merchant is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Merchant's end users to transmit or process, any Sensitive Data via the SaaS.

6.2 Merchant Account Data and Merchant Usage Data.

(a) Sensitive Data may be found in Merchant Account Data in the form of Subscriber Records containing passport or similar identifier data necessarily processed in order to receive services.

(b) Merchant Usage Data does not contain Sensitive Data.

Schedule 2

Jurisdiction Specific Terms

1. United States of America:

1.1 "US State Privacy Laws" means all state laws relating to the protection and processing of personal data in effect in the United

States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

1.2 The definition of "Applicable Data Protection Law" includes US State Privacy Laws.

1.3 The following terms apply where oneapp processes personal data subject to the CCPA:

(a) The term "personal information", as used in this Section 11.3, will have the meaning provided in the CCPA;

(b) oneapp is a service provider when processing Merchant Content. oneapp will process any personal information contained in Merchant Content only for the business purposes set forth in the Agreement, including the purpose of processing and processing activities set forth in this Addendum ("Purpose"). As a service provider, oneapp will not sell or share Merchant Content or retain, use, or disclose Merchant Content (i) for any purpose other than the Purpose, including retaining, using, or disclosing Merchant Content for a commercial purpose other than the Purpose, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Merchant and oneapp;

(c) oneapp will (i) comply with obligations applicable to it as a service provider under the CCPA and (ii) provide personal information with the same level of privacy protection as is required by the CCPA. Merchant is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the SaaS and its own processing of personal information;

(d) Merchant will have the right to take reasonable and appropriate steps to help ensure that oneapp uses personal information in a manner consistent with Merchant's obligations under the CCPA;

(e) oneapp will notify Merchant if it makes a determination that it can no longer meet its obligations as a service provider under the CCPA;

(f) Upon notice, Merchant will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of personal information;

(g) oneapp will provide reasonable additional and timely assistance to assist Merchant in complying with its obligations with respect to consumer requests as set forth in the Agreement;

(h) For any sub-processor used by oneapp to process personal information subject to the CCPA, oneapp will ensure that oneapp's agreement with such sub-processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors;

(i) oneapp will not combine Merchant Content that it receives from, or on behalf of, Merchant, with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless such combination is required to perform any business purpose as permitted by the CCPA, including any regulations thereto, or by regulations adopted by the California Privacy Protection Agency; and

(j) oneapp certifies that it understands and will comply with its obligations under the CCPA.

1.4 oneapp acknowledges and confirms that it does not receive Merchant Content as consideration for any SaaS provided to Merchant.