RESONATE DATA PROCESSING ADDENDUM

This DATA PROCESSING ADDENDUM (the "***DPA***") forms part of, and is subject to, the Resonate Master Subscription Agreement, Data Append Services and License Agreement or other written or electronic terms of service ("***Agreement***") between Resonate Networks, Inc. ("***Resonate***") and the legal entity executing identified as "Customer" in the applicable Agreement ("***Customer***", and together with Resonate, the "***Parties***"). All capitalized terms not defined in this DPA retain the meaning given in the Agreement.

1. DEFINITIONS.

1.1. **"*Transfer Safeguards*"** means appropriate safeguards for Transfer provided by Data Protection Laws, such as a decision of adequacy taken by, or contractual clauses (such as SCCs or UK SCCs) considered as appropriate by a data protection authority.

1.2. "***Authorized Affiliate***" means a Customer Affiliate not a Party to the Agreement that is either a Data Controller or Data Processor of Customer Personal Data Processed by Resonate.

1.3. "***Claims***" has the meaning ascribed to it in Section 3.4 of this DPA.

1.4. "***Consent Requests***" has the meaning ascribed to it in Section 9.2 of this DPA.

1.5. "***Customer Personal Data***" means Customer Data that it is Personal Data, regardless of whether Customer acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller with respect to such Personal Data.

1.6. "***Data Controller***" has the meaning given to it (and any other analogous terms) under Data Protection Laws (*e.g.*, "Business" as defined in the CCPA).

1.7. "***Data Processor***" has the meaning given to it (and any other analogous terms) under Data Protection Laws (*e.g.*, "Service Provider" as defined in the CCPA).

1.8. "***Data Protection Laws***" means all data protection and privacy laws applicable to the jurisdiction where Resonate provides the Services and the respective party in its role in the Processing of Personal Data under the Agreement, including: Regulation (EU) 2016/679 (General Data Protection Regulation or "**GDPR**"), the GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 ("**UK GDPR**"), California Consumer Privacy Act of 2018 ("**CCPA**"), California Privacy Rights Act of 2020 ("**CPRA**"), Connecticut Data Privacy Act ("**CTDPA**"), Virginia Consumer Data Protection Act ("**VCDPA**"), the Colorado Privacy Act ("**CPA**"), the Canadian Personal Information Protection and Electronic Documents Act, SC 2000, c 5, and Canada's Anti-Spam Legislation ("**CASL**").

1.9. "***Data Subject***" has the meaning given to Data Subject, Consumer, or any other analogous term under Data Protection Laws.

1.10. "***Data Subject Request***" means a request from a Data Subject to exercise any of its rights under Data Protection Laws.

1.11. *"**Documentation***" means: (a) the Agreement and any schedule, statement of work, order form, work order, or similar document agreed to by the parties describing the Services; (b) any written instructions provided by the parties regarding the provisioning or Processing of Customer Personal Data in connection with the Services; or (c) processes established by Resonate regarding data subject requests that comply with Data Protection Laws. Any reference to "Documentation" means only the applicable Documentation to which the provisions of this DPA relates.

1.12. "***Hosting Region***" has the meaning ascribed to it in Section 7.1 of this DPA.

1.13. "***Objection Period***" has the meaning ascribed to it in Section 4.3 of this DPA.

1.14. "***Personal Data***" has the meaning given to Personal Data, Personal Information, or any other analogous term under Data Protection Law.

1.15. "***Processing***" means any operation or set of operations performed on Personal Data or on sets of Persona Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, and dissemination; "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

1.16. "***Purposes***" means Resonate's provision of the Services or processing of Customer Personal Data as described in the Documentation.

1.17. "***SCCs***" means the Standard Contractual Clauses for data transfers between EU and non-EU countries, as issued and updated by the European Commission.

1.18. "***Security Incident***" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Personal Data.

1.19. "***Security Requirements***" means the information security measures set forth in the Agreement that Resonate must employ in providing the Services, as described in Resonate security documentation, found at https://support.resonate.com/hc/en-us/articles/13967485062295. Resonate may review and update its Security Requirements from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

1.20. "***Sensitive Data***" means Personal Data that is classified as sensitive or special categories of data under Data Protection Law, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, sex life or sexual orientation data.

1.21. "***Services***" means the services provided by Resonate to Customer, as described in the Documentation.

1.22. "***Sub-Processor***" means subcontractors (in the U.S.) and any other Data Processor engaged by Resonate or applicable Affiliate of Resonate to Process Customer Personal Data.

1.23. "***Transfer***" means the cross-border transfer of Personal Data.

1.24. "***UK SCCs***" means the international data transfer agreement for data transfers between UK and countries outside of the UK, as issued and updated by the Information Commissioner Office in the UK.

1.25. "***Usage Data***" means usage and operations data in connection with Customer's use of the Services, including login information, query logs, and metadata (*e.g.*, object definitions and properties).

2. **SCOPE AND APPLICABILITY OF THIS DPA.** This DPA applies to Customer Personal Data processed as part of the Services as a Data Processor. This DPA does not apply to Usage Data.

3. **ROLES AND SCOPE OF PROCESSING.**

3.1. Role of the Parties. As between Resonate and Customer, Resonate shall Process Customer Personal Data only as a Data Processor (or sub-processor) acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein, in each case regardless of whether Customer acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller (such third-party, the "***Third-Party Controller***") with respect to Customer Personal Data. To the extent any Usage Data is considered Personal Data under applicable Data Protection Laws, Resonate is the Data Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws. Neither Party shall instruct the other to take any action that would violate Data Protection Law. A Party shall promptly notify the other if, in its opinion, any instructions from the other Party violate this DPA, or if it can no longer comply with its obligations under this DPA. The Parties shall reasonably assist each other in meeting their respective obligations under Data Protection Laws. Both parties have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

3.2. Customer Instructions. Resonate will Process Customer Personal Data only for the Purposes. The Agreement, this DPA, and the Documentation set out the instructions to Resonate for all Processing of Customer Personal Data. Customer shall be responsible for any communications, notifications, costs, assistance or authorizations that may be required in connection with a third-party Data Controller of Customer Personal Data.

3.3. Restrictions on the Use of Customer Personal Data. Resonate shall not, and shall not authorize any third party to: (i) process, retain, use, sell, transfer, disclose, or otherwise share Customer Personal Data for any Purposes other than

as directed by Customer under this DPA, the Agreement, or any applicable Documentation; and/or (ii) combine Customer Personal Data with Personal Data that it receives from, or on behalf of, another person or persons, or collects on its own, except as directed by Customer for the Purposes and permitted by Data Protection Law.

3.4. Authorized Affiliates. Customer must communicate any Authorized Affiliate Processing instructions to Resonate. Customer is responsible for Authorized Affiliate compliance with this DPA. All acts or omissions of an Authorized Affiliate are considered the acts or omissions of Customer. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding, or otherwise against Resonate ("***Claim***"), all such Claims: (i) must be brought by Customer on behalf of the Authorized Affiliate, unless Data Protection Laws require Authorized Affiliate be a party; and (ii) are considered made by Customer and remain subject to any limitations on liability in the Agreement.

3.5. Processing of Personal Data.

(a) Resonate and Customer shall each, respectively, make appropriate use of the Services to ensure a level of security, including technical and organizational measures, appropriate to the nature and content of the Personal Data, such as encrypting, pseudonymizing, and backing-up Personal Data. Resonate and Customer shall respectively provide notice and obtain all consents, permissions, and rights or related legal basis necessary for to lawfully Process Personal Data.

(b) Certain Services result in disclosure of Personal Data to Customer (e.g., third-party audiences, custom identifiers, cookies data, mobile identifiers, Rapids, Abelite IDs, or other personal identifiers) by matching to or creating data from Customer Personal Data or providing data directly from another party. In such cases, Customer shall: (i) use the Personal Data only for the permitted Purpose; (ii) ensure that Customer's use of the Personal Data is consistent with this DPA and in compliance with Data Protection Laws; and (iii) upon request, provide Resonate with an accurate description of its use of the Personal Data, and certify to Resonate its use of the Personal Data complies with the Agreement, this DPA, the Documentation, and Data Protection Laws.

3.6. Details of Data Processing. Details of the Processing will be included in the Documentation. Otherwise, the following shall apply:

(a) *Subject Matter*. The subject matter of the Processing under this DPA is Customer Personal Data.

(b) *Frequency and Duration*. Notwithstanding expiry or termination of the Agreement or Documentation, Resonate will Process the Customer Personal Data continuously and until deletion of all Customer Personal Data.

(c) *Purpose*. Resonate will Process the Customer Personal Data for the Purpose.

(d) *Nature of the Processing*. Resonate will perform Processing as needed for the Purpose and to comply with Customer's Processing instructions as provided in accordance with the Agreement, Documentation, and this DPA.

(e) *Retention Period*. The period for which Customer Personal Data will be retained by Resonate and the criteria used to determine that period shall be determined by Customer during the term of the applicable Schedule via its use and configuration of the Service. Upon termination or expiration of the Schedule or Agreement as a whole, Customer may retrieve or delete all Customer Personal Data as set forth in the Agreement or Schedule. Customer Personal Data not deleted by Customer shall be deleted by Resonate promptly following: (i) expiration or termination of the Agreement or Schedule; and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement or Schedule.

(f) *Categories of Data Subjects*. The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion and may include, but are not limited to: (i) Customers, prospects, companies, business partners, and vendors of Customer (who are natural persons); (ii) Employees or contact persons of Customer's customers, prospects, business partners, and vendors; or (iii) Employees, agents, advisors, and freelancers of Customer (who are natural persons).

(g) *Categories of Personal Data*. The types of Customer Personal Data are determined by Customer, and may include:(i) contact data (such as name, address, phone number, alias, or title); (ii) identifiers (such as personal, government, online, device or mobile identifiers, cookie data, or IP address); (iii) attributes (such as demographic data, geographic location, account name); (iv) Employment data (such as employer, job title, or role); (v) network activity information (such as system, website, application, advertisement, or IT information); or (v) Financial information (such as credit card, account, or payment information). Customer Personal Data shall only include Sensitive Data if the Documentation authorizes, with specificity, the exchange of Sensitive Data and Customer has obtained the consents necessary to Process the Sensitive Data. If consent is not necessary, then Customer must have provided the Data Subject the opportunity to opt out of such Processing.

4. **SUB-PROCESSING.**

4.1. Authorized Sub-Processors. Resonate is authorized to engage its Affiliates as well as Resonate's current Sub-processors listed at https://support.resonate.com/hc/en-us/articles/13969443112087, as Sub-processors. Further details on the subject matter, nature and duration of the processing by such Sub-processors may be provided within the

Documentation.

4.2. Sub-Processor Obligations. Resonate must enter into a written agreement with each Sub-processor imposing the same obligations under this DPA to the extent applicable to the nature of the services provided by such Sub-processor. Sub-processors must use industry standard security measures designed to protect against a Security Incident, including appropriate organizational, contractual, technological, and managerial safeguards and necessary Transfer Safeguards. Upon written request, and subject to any confidentiality restrictions, Resonate shall provide Customer relevant information regarding Sub-processor agreements necessary under Data Protection Law. Resonate shall remain fully responsible to the Customer for the performance of the Sub-processor's obligations in accordance with its contract with Resonate. Resonate shall notify the Customer of any failure by the Sub-processor to fulfill its contractual obligations.

4.3. Changes to Sub-Processors**.** In advance of any proposed changes to its Sub-processors, resonate shall inform Customer in writing via a web-based subscription method for email notification accessible here: https://Resonate.com/legal/subprocessors. Customer shall subscribe to such notifications. Notification will include: (a) the name and address of the Sub-processor; (b) the nature, purpose, location and duration of the Processing; and (c) where applicable, the legal basis for the Transfer of the Customer Personal Data; and (e) the duration of the Processing. Customer has fourteen (14) days from receipt of notification ("***Objection Period***") to object to a new Sub-processor. Any objection must be provided to Resonate in writing and state the grounds on which the objection is based. Customer may not unreasonably withhold the approval of a Sub-processor. If no objection is received by the end of the Objection Period, the Sub-processor will be deemed approved by Customer. If it can be reasonably demonstrated to Resonate that the new Sub-processor is unable to Process Customer Personal Data in compliance with the terms of this DPA and Resonate cannot provide an alternative Sub-processor, or if the Parties are not otherwise able to achieve resolution, Customer, as its sole and exclusive remedy, may provide written notice to Resonate terminating those Services that cannot be provided by Resonate without the use of the new Sub processor. Resonate will refund Customer any prepaid unused fees for such Services as of the effective date of termination.

5. **SECURITY.**

5.1. Security Measures. Resonate shall implement and maintain appropriate technical and organizational security measures designed to preserve the security and confidentiality of the Customer Personal Data, when appropriate, such measures are further described in the Documentation. Such measures shall adhere to the Security Requirements.

5.2. Confidentiality. Resonate shall ensure that any person who is authorized by Resonate to Process Customer Personal Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3. No Assessment of Customer Personal Data by Resonate. Resonate shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for reviewing the information made available by Resonate relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

6. CUSTOMER AUDIT RIGHTS.

6.1. No more than once annually in the ordinary course, Customer may request documentation prepared by Resonate in the ordinary course of its business evidencing Resonate's compliance with this DPA. The audit scope may not extend beyond information applicable to Customer. Customer must share audit results with Resonate and any remediations based on the audit findings must be agreed to by Resonate. Audit findings and results are considered Resonate Confidential Information. The exercise of audit rights under the SCCs must adhere to this Section 6.

6.2. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/is on request.

7. DATA TRANSFERS.

7.1. Hosting and Processing Locations. Resonate will only host Customer Personal Data in the region(s) offered by Resonate and selected by Customer in the Agreement or as Customer otherwise configures via the Services (the "*Hosting Region*"). Customer is solely responsible for the regions from which it accesses the Customer Personal Data resulting in the transfer or sharing of Customer Personal Data by Customer. Resonate will not Process Customer Personal Data from outside the Hosting Regions except: (a) as reasonably necessary to provide the Services procured by Customer or (b) as necessary to comply with applicable law or binding order of a governmental body.

7.2. Transfer Description and Compliance Mechanisms. Any Transfer to a third country or an international

organization by Resonate shall be done on the basis of documented instructions from the Customer or in order to fulfill a specific requirement under applicable Data Protection Laws to which Resonate is subject. When such a Transfer occurs, the Parties shall establish the necessary Transfer Safeguards.

7.3. Transfer to a Sub processor. Customer agrees that, where resonate engages a Sub-processor in accordance with Clause 4. for carrying out specific processing activities (on behalf of the Customer) and those processing activities involve a Transfer, Resonate and the Sub-processor can ensure compliance with GDPR or UK GDPR by using SCCs or UK SCCs, provided the conditions for the use of those SCCs or UK SCCs are met.

8. SECURITY INCIDENT RESPONSE.

8.1. Security Incident Reporting. Insofar as reasonably practicable, Resonate shall assist Customer in meeting its obligations related to the security of processing personal data and notification of Security Incidents. If Resonate becomes aware of a Security Incident involving Customer Personal Data, Resonate shall notify Customer without undue delay and in accordance with notification timelines and requirements specified in the Security Requirements. Resonate shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

8.2. Security Incident Communications. Resonate shall provide Customer with timely information about the Security Incident, including the nature and consequences of the Security Incident, the measures taken or proposed by Resonate to mitigate or contain the Security Incident, the status of Resonate's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Communications with Customer in connection with a Security Incident are not an acknowledgment by Resonate of any fault or liability with respect to the Security Incident.

9. COOPERATION.

9.1. Customer Data Subject Requests. Resonate provides Customer with a number of mechanisms and controls that Customer may use to assist it in responding to Data Subject Requests, and Customer will be responsible for responding to any Data Subject Requests using the mechanisms and controls provided by Resonate and described in the supporting Documentation. If Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, Resonate shall (upon Customer's written request and taking into account the nature of the Processing) provide reasonable cooperation to assist Customer in responding to Data Subject Requests. If resonate receives a Data Subject Request related to Customer Personal Data, it shall notify Customer, if required by Data Protection Law, or otherwise direct the Data Subject to exercise a Data Subject Request directly with Customer.

9.2. Consumer Consent Requests. Resonate will provide mechanisms for Customer to receive signals indicating a consumer's processing instructions applicable to Resonate provided data, such as a signal indicating a consumer's consent to processing or choice to limit processing, opt out, or delete (collectively, "***Consent Requests***"). Upon receipt of any Consent Request from Resonate related to a data subject, Customer shall act in accordance with the consumer's expressed instructions as indicated by the Consent Request and any instructions found in the supporting Documentation.

9.3. Data Protection Impact Assessments. Resonate shall provide reasonably requested information regarding the Services to enable Customer to demonstrate compliance with Data Protection Laws and to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

9.4. Government, Law Enforcement, or Third-Party Inquiries. If either party receives any correspondence, inquiry, or complaint from any individual, supervisory authority, other relevant regulator, or other third party in connection to the Services, then the parties shall cooperate in good faith as necessary to enable that party to respond. If Resonate receives a demand to retain, disclose, or otherwise Process Customer Personal Data for any third party, including, but not limited to law enforcement or a government authority, then Resonate shall attempt to redirect the demand to Customer by providing Customer contact information to such third-party, or, if unable to redirect the demand, Resonate shall provide Customer reasonable notice of the demand as promptly as feasible. This section does not diminish Resonate's obligations under the SCCs with respect to access by public authorities.

9.5. Right to Suspend Services. If Resonate reasonably believes that Customer's use of the Services violates Resonate's privacy standards and practices, is unauthorized, or violates Data Protection Laws, Customer grants Resonate the right, upon notice, to take reasonable and appropriate steps to stop and remediate, including suspension of Services. Resonate will endeavor to provide a 10-day notice; however, suspension may occur contemporaneously with such notice if the violation jeopardizes Resonate's ability to provide Products to its other customers or exposes Resonate to a violation of law, potential fines, or civil liability. The notice shall include a description of the violation. Such action will not limit any of Resonate's other rights or remedies at law or in equity.

10. RELATIONSHIP WITH THE AGREEMENT.

10.1. Resonate may update this DPA from time to time, with such updated version posted to www.Resonate.com/legal, or a successor website designated by Resonate with an email notification also sent to Customer; provided, however, that no such update shall materially diminish the privacy or security of Customer Personal Data.

10.2. Each Party's liability (including liability for any regulatory penalties incurred by the other Party) arising out of or relating to this DPA or the SCCs remain subject to the limitations on liability in the Agreement.

10.3. The DPA does not benefit or create any right or cause of action on behalf of any third party, but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the SCCs).

10.4. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions as set forth in the Agreement.