DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the commercial agreement ("**Agreement**") which was executed by vcita Inc., vcita Systems Ltd. and/or its Affiliates ("**vcita**") and the person or entity whose details are indicated in the applicable online registration form or the Agreement ("**Customer**") to reflect the parties' agreement on the Processing of Customer Data (as defined below) as part of the provision of Services. vcita and customer may collectively be referred to herein as the "**Parties**" and each singularly as a "**Party**".

All capitalized terms not defined herein will have the meaning set forth in the Agreement, or under the applicable Privacy Laws and Regulations. All terms under the Agreement apply to this DPA, except that the terms of this DPA will supersede any conflicting terms under the Agreement. In the event of any conflict or inconsistency between this DPA and the EU SCCs, the EU SCCs will prevail.

In the course of providing the service to Customer pursuant to the Agreement ("**Service**"), vcita may Process Personal Data on behalf of Customer as a data processor ("**Customer Data**") subject to the terms of this DPA.

1. **DEFINITIONS**

1.1. "**Affiliate**" means any legal entity directly or indirectly controlling, controlled by or under common control with a party to the Agreement, where "control" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "**Data Controller**" and "**Data Processor**" will have the same meaning as under applicable Privacy Laws and Regulations and will include the terms "**Business**" and "**Service Provider**" and any similar term under applicable Privacy Laws and Regulations.

1.3. "**Data Subject**" means an identified or identifiable natural person; 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Data Subject includes Consumer as such term is defined under the CPRA and any similar terms under Data Privacy Laws and Regulations.

1.4. "**EU SCCs**" means the Standard Contractual Clauses pursuant to EU Commission Implementing Decision (EU) 2021/914.

1.5. "**Personal Data**" means information relating to a Data Subject. Personal Data includes Personal Information as such term is defined under the CPRA and any similar terms under Data Privacy Laws and Regulations.

1.6. "**Personnel**" means persons authorized by vcita to Process Customer's Personal Data.

1.7. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, and includes any similar terms under Data Privacy Laws and Regulations.

1.8. "**Privacy Laws and Regulations**" means the following laws, including any applicable regulations, amendments and superseding laws related thereto: (**A**) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**"); (**B**) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (**C**) the California Consumer Privacy Act of 2018 Cal. Civil Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 ("**CPRA**"), and any other applicable consumer privacy laws of a US state ("**US Privacy Laws**"); (**D**) ; the Brazilian General Data Protection Law, officially named as Brazil's Lei Geral de Proteção de Dados ("**LGPD**"); (**E**) the Australian Privacy Act 1988 (Cth) No. 119 1988 (as amended); (**F**) the Swiss Federal Act on Data Protection of 19 June 1992 (Status as of 1 March 2019) as replaced by its amendment of September 25, 2020 (effective as of September 1, 2023) ("**FADP**"); and, (**G**) the Israeli Protection of Privacy Law, 5741-1981 ("**PPL**").

1.9. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available,

alignment or combination, blocking, erasure or destruction, and includes any similar terms under Data Privacy Laws and Regulations

1.10. "**Third Country**" means a country outside the European Economic Area ("**EEA**"), the UK or Switzerland, which was not acknowledged by the EU Commission, a UK Secretary of State or the FDPIC (as applicable) as providing an adequate level of protection in accordance with Article 45(3) of the GDPR, Article 45 of the UK GDPR or the equivalent, and with respect to Israel will include any country outside of the territory of Israel.

2. DATA PROCESSING

2.1. **Scope and Roles**. This DPA applies when Customer Data is Processed by vcita as part of vcita's provision of the Service to Customer. In this context, Customer is the Data Controller or Data Processor (as applicable) and vcita is the Data Processor.

2.2. **Subject Matter, Duration, Nature and Purpose of Processing.** vcita Processes Customer Data as part of providing Customer with the Service, pursuant to the specifications and for the duration under the terms of the Agreement, as further specified under **ANNEX 1** to this DPA.

2.3. **Instructions for vcita's Processing of Customer Data**. Customer instructs vcita to Process Customer Data for the following purposes: (**A**) Processing in accordance with the Agreement and applicable order forms, including, without limitation to provide, operate, control, supervise, and safeguard the Services – all integral parts of the provision of the Service to Customer; and, (**B**) Processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement and comply with applicable Privacy Laws and Regulations. Processing outside the scope of this DPA (if any) will require prior written agreement between vcita and Customer on additional instructions for Processing, including agreement on any additional fees Customer will pay to vcita for carrying out such instructions. Customer undertakes to provide vcita with lawful instructions only. vcita will inform Customer if in its opinion an instruction violates any provision under Privacy Laws and Regulations and will be under no obligation to follow such instruction, until the matter is resolved in good-faith between the Parties.

2.4. **US Specific Provisions**. To the extent that US Privacy Laws apply to the Processing of Customer Data by vcita, the following provisions will also apply to such Processing: (**1**) Customer and vcita acknowledge that Customer Data is disclosed to vcita only for the limited Business Purpose of providing Customer with the Service (the "**Purpose**"), vcita will only use such data for those limited and specified purposes, and Customer is not selling Customer Data to vcita; (**2**) vcita will comply with all provisions under US Privacy Laws applicable to vcita, including with respect to providing the same level of protection to privacy as required under the CPRA by a Business and will notify Customer no later than within five (5) business days after determining that vcita can no longer meet its obligations under US Privacy Laws; (**3**) vcita will not Sell of Share (within the meaning of such terms under US Privacy Laws) Customer Data, and will not, unless otherwise permitted under US Privacy Laws, retain, use, or disclose Customer Data: (**A**) for any purposes other than those specified under this DPA; (**B**) for any commercial purpose other than the Purpose, including in providing services to other customers of vcita; or, (**C**) outside the direct business relationship between Customer and vcita; (**4**) vcita will not retain use, or disclose Customer Data outside the direct business relationship between the parties and will not combine Customer Data with Personal Data that vcita receives from, or on behalf of, another third party, including other vcita customers, or with Personal Data that vcita collects from its own interaction with Data Subjects; and, (**5**) Customer may take reasonable and appropriate steps to ensure that vcita uses Customer Data in a manner consistent with Customer's obligations under US Privacy Laws, and may, upon notice, take reasonable and appropriate steps to stop and remediate vcita's unauthorized use of Customer Data; and, (**6**) Customer will inform vcita of any consumer request made pursuant to US Privacy Laws that vcita must comply with and will provide vcita the information necessary for vcita to comply with the request.

2.5. Customer warrants and represents that it is and will remain duly and effectively authorized to give the instruction set out in Section 2.3 and any additional instructions as provided pursuant to the Agreement and/or in connection with the performance thereof, on behalf of itself and each relevant Customer Affiliate, at all relevant times and at least for as long as the Agreement is in effect and for any additional period during which vcita and/or its Affiliates are lawfully processing Customer Data.

2.6. Customer undertakes to provide all necessary notices to Data Subjects and receive all necessary permissions and consents (including to the extent required under applicable Privacy Laws and Regulations to the international transfer of Customer Data outside of the country where such data originates from), or otherwise secure the required lawful ground of Processing, as necessary for vcita to process Customer Data

on Customer's behalf under the terms of the Agreement and this DPA, pursuant to the applicable Privacy Laws and Regulations.

2.7. To the extent required under the applicable Privacy Laws and Regulations, Customer will appropriately receive and document the Data Subjects' notices and consents or will otherwise secure other applicable lawful grounds of Processing.

2.8. Customer may only provide vcita and/or its Affiliates, or otherwise have vcita (or anyone on its behalf) Process, such Customer Data types and parameters which are explicitly permitted under Customer's Privacy Policy ("**Permitted Customer Data**"). Solely Customer (and not vcita and/or its Affiliates) will be liable for any data which is provided or otherwise made available to vcita or anyone on its behalf in excess of the Permitted Customer Data ("**Excess Data**"). vcita's obligations as Processor under the Agreement or this DPA shall not apply to any such Excess Data.

3. **ASSISTANCE**. Taking into account the nature of the Processing, vcita will assist Customer by appropriate technical and organizational measures, insofar as this is possible, to fulfil Customer's obligation to respond to requests for exercising Data Subjects' rights, as required under applicable Privacy Laws and Regulations. vcita will further reasonably assist Customer in ensuring compliance with Customer's obligations under applicable Privacy Laws and Regulations, including obligations in connection with the security of Processing, notification of a Personal Data Breach to supervisory authorities and affected Data Subjects, Customer's data protection impact assessments and Customer's prior consultation with supervisory authorities, in relation to vcita's Processing of Customer Data under this DPA. Except for negligible costs, Customer will reimburse vcita with costs and expenses incurred by vcita in connection with the provision of assistance Customer under this DPA.

4. **DATA SUBJECT RIGHTS**. To the extent legally permitted, vcita will promptly notify Customer if vcita receives a request from a Data Subject, who's Personal Data is included in Customer Data, or a request by the Data Subject's legal guardians, to exercise the Data Subject's right to access, correct, amend, or delete Personal Data related to the Data Subject, or to exercise such other personal right that the Data Subject is entitled to pursuant the applicable requirements under Privacy Laws and Regulations.

5. **VCITA PERSONNEL**. Vvita will ensure that vcita's access to Customer Data is limited only to Personnel who require such access to perform the Agreement. vcita will impose appropriate contractual obligations upon its Personnel engaged in the Processing of Customer Data, including relevant obligations regarding confidentiality, data protection, and data security. vcita will ensure that such Personnel are informed of the confidential nature of Customer Data, have received appropriate training in their responsibilities, and have executed written confidentiality agreements under terms at least as protective as the terms of this DPA. vcita will ensure that such confidentiality agreements survive the termination of the employment or engagement of its Personnel.

6. **SUB-PROCESSORS**. vcita may engage third-party service providers to process Customer Data on behalf of Customer ("**Sub-Processors**"). Customer hereby provides vcita with a general authorization to engage its Sub-Processors listed under **ANNEX 3**. All Sub-Processors have entered into written agreements with vcita that bind them by substantially the same material obligations under this DPA. vcita may engage with a new Sub-Processor ("**New Sub-Processor**") to Process Customer Data on Customer's behalf. Customer may object to the Processing of Customer Data by the New Sub-Processor, for reasonable and explained grounds, within five (5) business days following vcita's written notice to Customer of the intended engagement with the New Sub-Processor. If Customer timely sends vcita a written objection notice, the parties will make a good-faith effort to resolve Customer's objection. In the absence of a resolution, vcita will make commercially reasonable efforts to provide Customer with the same level of Service, without using the New Sub-Processor to Process Customer Data. Where a Sub-Processor fails to fulfil its data protection obligations in connection with the Processing of Customer Data under this DPA, vcita will remain fully liable to Customer for the performance of that Other Processor's obligations.

7. **ONWARD AND TRANS-BORDER DATA TRANSFERS**. Transfers of Customer Data to a Third Country by vcita or by vcita's Sub-Processors are subject to the data transfer requirements under **ANNEX 4**.

8. **INFORMATION SECURITY**. vcita will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Customer Data pursuant to the vcita technical and organizational measures under **ANNEX 2** to this DPA.

9. **AUDIT AND DEMONSTRATION OF COMPLIANCE**. vcita will make available to Customer all information reasonably necessary to demonstrate compliance with vcita's obligations under applicable Privacy Laws and Regulations. vcita will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, in relation to vcita's obligations under this DPA. vcita may satisfy the audit obligation under this section

by providing Customer with attestations, certifications and summaries of audit reports conducted by accredited third party auditors. Other audits by Customer are subject to the following terms: (**A**) the audit will be pre-scheduled in writing with vcita, at least forty-five (45) days in advance and will be performed not more than once a year (unless the audit is required by a competent supervisory authority); (**B**) a third-party auditor will execute a non-disclosure and non-competition undertaking toward vcita; (**C**) the auditor will not have access to non-Customer Data; (**D**) Customer will make sure that the audit will not interfere with or damage vcita's business activities and information and network systems; (**E**) Customer will bear all costs and expenses related to the audit; (**F**) the auditor will first deliver a draft report to vcita and allow vcita reasonable time and no less than ten (10) business days, to review and respond to the auditor's findings, before submitting the report to the Customer; (**G**) Customer will treat the auditor's report as vcita's Confidential Information and will only receive the auditor's report, with vcita's comments, without any vcita 'raw data' materials, will keep the audit results in strict confidentiality and will use it solely for the specific purposes of the audit under this DPA; and (**H**) as soon as the purpose of the audit is completed, Customer will permanently and completely dispose of all copies of the audit report.

10. **PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION**. vcita maintains security incident management and breach notification policies and procedures and will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Data which vcita, or any of vcita's Sub-Processors, Process. vcita's notice will at least: (**A**) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Data records concerned; (**B**) communicate the name and contact details of the vcita's Data Protection Team, which will be available to provide any additional available information about the Personal Data Breach; (**C**) describe the likely consequences of the Personal Data Breach; (**D**) describe the measures taken or proposed to be taken by vcita to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. vcita will work diligently, pursuant to its incident management and breach notification policies and procedures to promptly identify and remediate the cause of the Personal Data Breach and will promptly inform Customer accordingly.

11. **DELETION OF CUSTOMER DATA**. Within reasonable time after the end of the provision of the Service and upon Customer request, vcita will return Customer Data to Customer or delete such data, including by de-identifying or anonymizing thereof, unless otherwise permitted under applicable Privacy Laws and Regulations.

12. **DISCLOSURE TO COMPETENT AUTHORITIES**. vcita may disclose Customer Data if required by a subpoena or other judicial or administrative order, or if otherwise required by law, or vcita deems the disclosure necessary to protect the safety and rights of any person, or the general public.

13. **ANONYMIZED AND AGGREGATED DATA**. vcita may process data based on extracts of Customer Data on an aggregated and non-identifiable form for vcita's legitimate business purposes, including for testing, development, controls, and operations of the Service, and may share and retain such data at vcita's discretion, provided that such data cannot reasonably identify a Data Subject.

14. **TERM**. This DPA will commence on the same date that the Agreement is made effective and will continue until the Agreement is expired or terminated, pursuant to the terms therein, provided that vcita's obligations hereunder with respect to Customer Data will continue to apply for as long as vcita continues to Process Customer Data.

15. **VCITA DATA PROTECTION TEAM**. vcita's data protection team is responsible to ensure adherence to the terms of this DPA and can be reached at privacy@vcita.com.

16. **DISPUTE RESOLUTION**. Each Party will create an escalation process and provide a written copy to the other Party within five (5) business days of any dispute arising out of or relating to this DPA. The escalation process will be used to address disputed issues related to the performance of this DPA, including but not limited to technical problems. The Parties agree to communicate regularly about any open issues or process problems that require prompt and accurate resolution as set forth in their respective escalation process documentation. The Parties will attempt in good faith to resolve any dispute arising out of or relating to this DPA, before and as a prior condition for commencing legal proceedings of any kind, first as set forth above in the escalation process and next by negotiation between executives who have authority to settle the controversy and who at a higher level of management than the persons with direct responsibility for administration of this DPA. Any Party may give the other Party written notice of any dispute not resolved in the normal course of business. Within five (5) business days after delivery of the notice, the receiving Party shall submit to the other a written response. The notice and the response will include (a) a statement of each Party's position and a summary of arguments supporting that position and (b) the name and title of the executive who will represent that Party and of any other person who will accompany the executive. Within fifteen (15) business days after delivery of the disputing Party's notice, the executives of both Parties shall meet at a mutually

acceptable time and place, including telephonically, and thereafter as often as they reasonably deem necessary, to attempt to resolve the dispute. All reasonable requests for information made by one Party to the other will be honored. All negotiations pursuant to this clause are confidential and will be treated as compromise and settlement negotiations for purposes of applicable rules of evidence.

17. **MISCELLANEOUS**. Any alteration or modification to this DPA will not be valid unless made in writing and executed by duly authorized personnel of both parties. If any term or provision under this DPA is declared invalid, illegal or unenforceable, all remaining provisions will continue in full force and effect and any invalid provisions will be replace by those valid provisions which achieve essentially the same objectives.

* * *

ANNEX 1
DETAILS OF PROCESSING
(ALSO SERVES AS ANNEX I TO THE EU SCCS)

A. **LIST OF PARTIES**

Data Controller (Exporter): Customer, whose name, address, and contact details are as detailed in the Agreement. Customer assumes the role of a Data Controller.

Data Processor (Importer): vcita Inc. ("**vcita**"), whose name, address, and contact details are as detailed in the Agreement. Vcita assumes the role of a Data Processor.

Activities Relevant to the Data Transferred Under the EU SCCs: provision of the Service under the Agreement.

Contact Persons. The Parties' contact persons are as detailed in the Agreement or the applicable order form.

To the extent required under the EU SCCs, Customer's and vcita's signatures on the Agreement applies herein.

B. **DESCRIPTION OF THE PROCESSING (TRANSFER)**

Categories of data subjects whose personal data is processed\transferred

Customer's customers, employees, contractors and service providers.

Categories of personal data transferred

Users' names, contact details, log-in details, billing information, online usage information, browser information.

Any information uploaded or provided by Customer and/or Customer's users as part of the Service, subject to Customer's discretion.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

Any information uploaded by Customer's users to the Service, subject to Customer's discretion.

The frequency of the transfer

Continuous basis for the duration of the Agreement.

Nature of the processing

All operations such as collection, recording, organization, structuring, storage, adaptation or alteration, updating, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means), etc.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained during the term of the Agreement and will be deleted in accordance with the terms therein.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter of the processing is Customer's Personal Data, the nature of the Processing is the performance of the Service under the Agreement and as detailed above and the duration of the Processing is the term of the Agreement.

C. **COMPETENT SUPERVISORY AUTHORITY**

Where the data exporter is established in an EU Member State: The supervisory authority of such EU Member State shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1): The supervisory authority of the Member State in which the representative is established shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2): The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent supervisory authority.

* * *

ANNEX 2

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

(ALSO SERVES AS ANNEX II TO THE EU SCCS)

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The technical and organizational measures (TOMs) provided below apply to all standard service offerings provided by vcita, except where the Customer is responsible for implementing technical and organizational measures to secure its data. Evidence of the measures implemented and maintained by vcita security may be presented in the form of up-to-date certifications from independent bodies upon receipt of a written request from the Customer.

These measures are commercially reasonable and are aligned with industry standard technical and organizational measures, to protect personal data. These measures are consistent with applicable laws and meet the standard of protection appropriate to the risk of processing Personal Data in the course of providing vcita's services. vcita will regularly carry out, test, review and update all such measures.

These measures will be subject to technical progress and future developments of vcita's services. Accordingly, vcita will be permitted to implement alternative adequate measures. In such event, the security level may not be lower that the measures memorialized hereto. Material changes will be coordinated with the relevant Data Controller(s) and will be documented.

Security Management

vcita maintains a written information security management system (ISMS), in accordance with this Annex, that includes policies, processes, enforcement and controls governing all storage/processing/transmitting of Personal Data, designed to:

(a) secure Personal Data against accidental or unlawful loss, access or disclosure;

(b) identify reasonably foreseeable and internal risks to security and authorized access to Customer's network; and

(c) minimize security risks, including through risk assessment and regular testing.

Secure Networks and Systems

vcita has installed and maintains a firewall configuration to protect Personal Data that controls all traffic allowed between Customer's (internal) network and untrusted (external) networks, as well as traffic into and out of more sensitive areas within its internal network. This includes current documentation, change control and regular reviews.

vcita does not use vendor-supplied defaults for system passwords and other security parameters on any system and has developed configuration standards for all system components consistent with industry-accepted system hardening standards.

Protection of Personal Data

vcita keeps Personal Data storage to a minimum and implements data retention and disposal policies to limit data storage to that which is necessary, in accordance with the needs of its customers.

vcita uses strong encryption and hashing for Personal Data anywhere it is stored. vcita has documented and implemented all necessary procedures to protect (cryptographic) keys used to secure stored Personal Data against disclosure and misuse. All transmission of Personal Data across open, public networks is encrypted using strong cryptography and security protocols.

Vulnerability Management Program

vcita protects all systems against malware and regularly updates anti-virus software or programs to protect against malware – including viruses, worms, and Trojans horses. Anti-virus software is used on all systems commonly affected by malware to protect such systems from current and evolving malicious software threats.

Access Controls

vcita maintains access controls and policies to manage what access is allowed to the network from each network connection and user, including the use of firewalls, VPN or functionally equivalent technology and authentication controls.

vcita strictly restricts access to Personal Data by business need-to-know to ensure that critical data can only be accessed by authorized personnel. This is achieved by:

(a) Limiting access to system components and Personal Data to only those individuals whose job requires such access; and
(b) Establishing and maintaining an access control system for systems components that restricts access based on a user's need to know, with a default "deny-all" setting.
(c) vcita identifies and authenticates access to all systems components by assigning a unique identification to each person with access. This ensures that each individual is uniquely accountable for their actions and any actions taken on critical data and systems can be traced to known and authorized users and processes.
(d) User authentication utilizes at least passwords that have to meet complexity rules, need to be changed on a regular basis and are cryptographically secured during transmission and storage on all system components.
(e) All individual and administrative access and all remote access use multi-factor authentication.

Contingency Planning

Network infrastructure relies on a secure cloud service platform with flexible capacity to ensure reliability and resilience.

Fault tolerance: backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Procedures governing backup jobs and schedules are implemented including contingency and disaster recovery plans covering computer facilities and critical applications and document repositories.

Physical Security Protections

All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities.

Any physical access to data or systems that house Personal Data are appropriately restricted using appropriate entry controls and procedures. Access to sensitive areas is controlled and includes processes for authorization based on job function and access revocation for personnel and visitors.

Media and backups are secured and (internal and external) distribution is strictly controlled. Media containing Personal Data no longer needed for business or legal reasons is rendered unrecoverable or physically destroyed.

Incident management

vcita has a formal procedure for managing data breach and data protection incidents; formal incident reporting and escalation procedures have been implemented. Information security incidents and vulnerabilities are reported as quickly as possible to the IT department and CISO.

Continued Evaluation.

vcita conducts periodic reviews of the security of its network and adequacy of its information security program as measured against industry security standards and its policies and procedures.

vcita continually evaluates the security of its network to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

ANNEX 3

LIST OF SUB-PROCESSORS

(TO THE EXTENT REQUIRED – ALSO SERVES AS ANNEX III TO THE EU SCCS)

Name of Other Processor	Description of the Processing	Location
Ada Support Inc.	Support Services (for specific Customers only)	Canada/USA
AWS	Data center	USA
Cloudinary	Images data center	USA
DataDog	Log monitoring	USA
Fullcontact	Data enrichment	USA
Fullstory	User activity monitoring	USA
Google	Marketing Analytics; Captcha	USA
Justt	Chargeback management	USA
Looker	Analytics	USA
Mixpanel	Analytics	USA
Nexmo/Vonage Sent	SMS Delivery	USA
OpenAI	AI services	USA
Pendo	In-app user guidance	USA
Racksapce	Documents data center	USA
Recurly	Financial transaction gateway	USA
Rivery	ETL Platform	USA
SendGrid	Email Delivery	USA
Snowflake	Data base	USA
Stichdata	ETL Platform	USA
Worknet Inc.	AI powered Support Services	USA
Zapier	Platform integration	USA
Zendesk	Support Management	USA
Zoom	Phone and recording system	USA

* * *

ANNEX 4
CROSS BORDER CUSTOMER DATA TRANSFER TERMS

1. **DEFINITIONS**. Capitalized terms not defined herein will have the meaning set forth in the DPA or under Privacy Laws and Regulations.

1.1. "**Adequacy Recognition**" means, a decision by a competent authority of a country, or statutory provisions, that recognize another country as providing an adequate level of protection to Personal Data, as determined pursuant to the Privacy Laws and Regulations applicable to the country that issued the decision or enacted such statutory provisions, and in accordance with such decision or statutory provisions, the transfer of Personal Data to such other recognized country is permitted without additional measures related to the transfer of the Personal Data.

1.2. "**DTRs**" mean the Protection of Privacy Regulations (Transfer of Data to Databases Abroad), 5761-2001.

1.3. "**EU SCCs**" means the Standard Contractual Clauses pursuant to EU Commission Decision C(2021)3972.

1.4. "**IDTA**" means the International Data Transfer Agreement, issued by the ICO in accordance with section 119A of the Data Protection Act 2018, or any other applicable standard contractual clauses issued, approved, or otherwise recognized by the ICO.

1.5. "**Swiss SCCs**" means the applicable standard contractual clauses issued, approved, or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**").

1.6. "**Statutory Transfer Agreement**" means statutory provisions enacted pursuant to Privacy Laws and Regulations, which establish binding terms for cross-border transfer of Personal Data from one jurisdiction to another, including where applicable under Privacy Laws and Regulations, through access to Personal Data from the non-transferring territory, which can be executed between the transferring and the recipient parties to facilitate the lawful cross-border transfer of Personal Data, including where applicable the EU SCCs.

1.7. "**Transferred Data**" means:

1.7.1. GDPR-governed Customer Data transferred outside the EEA ("**EU Transferred Data**");

1.7.2. UK-GDPR governed Customer Data transferred outside the UK ("**UK Transferred Data**");

1.7.3. FADP-governed Customer Data transferred outside of Switzerland ("**Swiss Transferred Data**"); and,

1.7.4. PPL-Governed Customer Data transferred outside of the territory of Israel ("**IL Transferred Data**").

1.8. "**UK Addendum**" means the UK addendum published by the Information Commissioner's Office's ("**ICO**") in accordance with section 119A(1) of the Data Protection Act of 2018, incorporating the EU SCCs.

2. **GENERAL**. Customer hereby consents, authorizes, and instructs vcita to Transfer Customer Data outside of the country where such data originated from. Transfers under the Agreement and DPA that are subject to Privacy Laws and Regulations that mandate a Transfer measure to facilitate the lawful Transfer of Customer Data will be made in accordance with the following provisions:

2.1. **Transfers to Adequate Countries**. When Transferred to countries holding an Adequacy Recognition, the Parties agree that Customer Data will be Transferred subject to such recognition.

2.2. **Transfers to Non-Adequate Countries**. When Transferred to countries that do not hold an Adequacy Recognition, or where such recognition is invalidated by the competent regulator, Customer Data will be Transferred under the applicable Statutory Transfer Agreement, and in accordance with the provisions of section 3 below.

3. **SPECIFIC PROVISIONS**. Transfers of Transferred Data to Third Countries will be made in accordance with the following provisions:

3.1. **EU Transferred Data**. Transfers of EU Transferred Data to a Third Country will be made under the EU SCCs, giving effect to module 2 or 3 as applicable, which is incorporated by reference to this DPA, as follows: (**A**) in Clause 7, the optional docking clause will apply; (**B**) if applicable – in clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes will be as set out in Section 6 of the DPA; (**C**) in clause 11, the optional language will not apply; (**D**) in clause 17, Option 1 will apply, and the EU SCC will be governed by the Irish law; (**E**) in clause 18(b), disputes will be resolved before the courts of Ireland; and, (**F**) Annexes (I)-(II) to the EU SCCs will be completed with the relevant details in **ANNEXES 1-3** to the DPA.

3.2. **UK Transfers**. Transfers of UK Transferred Data to a Third Country will be made: (**A**) in accordance with the EU SCCs as detailed in section 3.1 above, as amended by the UK Addendum, which is incorporated by reference to this DPA, with the necessary changes made as detailed in sections 12-15 to the UK Addendum; or, (**B**) if the EU SCCs as implemented above cannot be used to lawfully Transfer UK Transferred Data, the IDTA will instead be incorporated by reference and will form an integral part of this DPA, and will apply to Swiss Transferred Data. In such case, the relevant Annexes of the IDTA will be populated using the information contained in **ANNEXES 1-3**.

3.3. **Swiss Transfers**. Transfers of Swiss Transferred Data to a Third Country will be made: (**A**) in accordance with the EU SCCs as detailed in section 3.1 above, as recognized by the FDPIC on August 27, 2021, with the following modifications: (**1**) references to 'EU', 'Union', 'Member State' and 'Member State law' will be interpreted as references to 'Switzerland', and 'Swiss law', as applicable; and, (**2**) references to 'Competent supervisory authority' and 'Competent courts' will be interpreted as references to the FDIPC and Competent courts in Switzerland; or, (**B**) if the EU SCCs as implemented above cannot be used to lawfully Transfer Swiss Transferred Data in compliance with the FADP, the Swiss SCCs will instead be incorporated by reference, will form an integral part of this DPA, and will apply to Swiss Transferred Data. In such case, the relevant Annexes of the Swiss SCCs will be populated using the information contained in **ANNEXES A-B**.

3.4. **IL TRANSFERS**. Transfers of IL Transferred Data to a Third Country will be governed by the PPL and the DTRs. vcita will transfer Customer Data outside of Israeli territory in reliance on the Customer's obligation to secure the Data Subjects' consent to such transfers under section 3 to the DPA. If the Customer has failed to secure the appropriate consents from applicable Data Subjects to the transfer of Customer Data related to them outside of Israel, vcita will transfer Customer Data under one of the following conditions: (**1**) Customer Data is transferred to a country which is a party to the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108); or, (**2**) Customer Data is transferred to a country which receives data from Member States of the European Community under the same terms of acceptance (e.g., adequacy recognition, binding corporate rules, standard contractual clauses, etc.), which will be the EU SCCs, as implemented under section 3.1 above.

4. **SUPPLEMENTAL MEASURES FOR EEA TRANSFERRED DATA**. In accordance with Article 46 of the GDPR, the EU SCCs and guidelines published by the European Data Protection Board (EDPB), and without prejudice to any provisions of the DPA or this Annex, vcita undertakes to implement the following organizational and technical safeguards, in addition to the safeguards mandated by the EU SCCs, to ensure the required adequate level of protection to EU, UK, and Swiss Transferred Data:

4.1. **Technical and Organizational Measures**. vcita will implement and maintain the technical and organizational measures, as specified in **ANNEX 2**, which is attached and incorporated by reference to this DPA, with a purpose of protecting the Customer Data against any processing for national security or other government purposes that go beyond what is necessary and proportionate in a democratic society, considering the type of processing activities under the Agreement and relevant circumstances.

4.2. **Contractual Measures**. For the purposes of safeguarding Customer Data when any Third Country's government or regulatory authority requests access to such data ("**Request**"), and unless required by a valid court order or if otherwise vcita may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to Customer Data, or where the access is requested in the event of imminent threat to lives, vcita will: (**A**) not purposefully create back doors or similar programming that could be used to access Customer Data; (**B**) not provide the source code or encryption keys to any government agency for the purpose of accessing Customer Data; (**C**) upon Customer's written request, provide reasonable available information about the requests of access to Customer Data by government agencies vcita has received in the 6 months preceding to Customer's request; and, (**D**) notify Customer upon receiving a request by a government agency to access Customer Data to enable Customer to take necessary actions,

communicate directly with the relevant authority and to respond to the request. If vcita is prohibited by law to notify the Customer of such request, vcita will make reasonable efforts to challenge such prohibition through judicial action or other means at Customer's expense and, to the extent possible, will provide only the minimum amount of information necessary.

5. **FUTURE ADEQUACY**. As applicable, if: (**A**) an Adequacy Recognition is invalidated or otherwise terminated by the relevant competent authority; (**B**) the Statutory Transfer Agreement (including the EU SCCs) is invalidated or is no longer in effect; or (**C**) any other Transfer safeguard used for the Transfer of Customer Data under the DPA is no longer in effect for any reason, then vcita will take such alternative lawful measures, as may be available and applicable, to continue facilitating the lawful Transfer of Customer Data by vcita, vcita's Sub-Processors, vcitas' New Sub-Processors, or equivalents thereof.