EU Data Processing Addendum

This Data Processing Addendum (“DPA”) forms a part of Customer Terms of Service found at https://www.cliniko.com/policies/terms (the **“Agreement”**).

By accepting the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and Controller Affiliates. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services under the Agreement, Red Guava may Process Customer Data (such terms defined below) on behalf of Customer and where Red Guava Processes such Customer Data on behalf of Customer, the Parties agree to comply with the terms and conditions in this DPA in connection with such Customer Data.

How this DPA applies to the Customer and its Affiliates

This DPA is an addendum to and forms part of the Agreement. In such case, the Red Guava entity that is party to the Agreement is party to this DPA.

1. Definitions

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Authorised User” define as any person who is authorised by Red Guava to use the Services.

“Controller Affiliate” means any of Customer's Affiliate(s) (a) (i) that are subject to applicable Data Protection Laws, and (ii) permitted to use the Services pursuant to the Agreement between Customer and Red Guava, but are not a “Customer” as defined under the Agreement, (b) if and to the extent Red Guava processes Customer Data for which such Affiliate(s) qualify as the Controller.

“Customer” means if you are representing an entity, that entity, otherwise, means you as an individual.

“Customer Data” means all Personal Data Processed by Red Guava (or its appointed Sub-processors) on behalf of Customer, pursuant to the provision of the Services.

“Data Protection Laws” means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area and their member states, and Switzerland, applicable to the Processing of Personal Data under the Agreement, and “**Controller**”, “**Data Subject**”, “**Personal Data**”, “**Processing**”, “**Processor**” and “**Supervisory Authority**” shall have the meanings set out in Data Protection Laws (and related terms such as “**Processed**” shall have corresponding meanings).

“Red Guava” means Red Guava Pty. Ltd., a company incorporated in Melbourne, Australia, and constituted under the laws of Australia.

“Security Practices Datasheet” means Red Guava’s Security Practices Datasheet, as updated from time to time, and currently available at https://cliniko.com/security.

“Services” means the provision of the Cliniko software application and related platform, and services related thereto (such as customer support).

“Standard Contractual Clauses” means module two of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by European Commission decision of 4 June 2021 and published under document number C/2021/3972.

“Sub-processor” means any entity engaged by Red Guava to Process Customer Data in connection with the Services.

2. Processing of personal data

2.1. **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Customer Data, Customer is the Controller, Red Guava is the Processor and that Red Guava will engage Sub-processors pursuant to the requirements set forth in Section 4 “Sub-processors” below.

2.2. **Customer’s Processing of Personal Data.** Customer shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3. **Red Guava’s Processing of Customer Data.** As Customer’s Processor, Red Guava shall only Process Customer Data for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Authorised Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer from time to time (e.g., via email or support tickets) that are consistent with the terms of the Agreement (individually and collectively, the **“Purpose”**). Red Guava acts on behalf of and upon the instructions of Customer in carrying out the Purpose.

2.4. **Details of the Processing.** The subject-matter of Processing of Customer Data by Red Guava is as described in the Purpose in Section 2.3. The duration of the Processing, the nature and purpose of the Processing, the types of Customer Data

and categories of Data Subjects Processed under this DPA are further specified in Exhibit A (Description of Processing Activities) to this DPA.

3. Rights of data subjects

3.1. **Data Subject Requests.** Red Guava shall, to the extent legally permitted, promptly notify Customer if Red Guava receives any requests from a Data Subject to exercise the following Data Subject rights in relation to Customer Data: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a **"Data Subject Request"**). Taking into account the nature of the Processing, Red Guava shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Red Guava shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Red Guava is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Red Guava's provision of such assistance, including any fees associated with provision of additional functionality.

4. Sub-processors

4.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Red Guava's Affiliates may be retained as Sub-processors through written agreement with Red Guava and (b) Red Guava and Red Guava's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. As a condition to permitting a third-party Sub-processor to Process Customer Data, Red Guava or a Red Guava Affiliate will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. Customer acknowledges that Red Guava is located in Australia and is involved in providing the Services to Customer directly. Customer agrees to enter into the Standard Contractual Clauses set out in Exhibit B and acknowledges that Sub-processors may be appointed by Red Guava in accordance with Clause 9 of Exhibit B.

4.2. **List of Current Sub-processors and Notification of New Sub-processors.** A current list of Sub-processors for the Services, including the identities of those Sub-processors and their country of location, is accessible via https://help.cliniko.com/privacy/data-processing/cliniko-subprocessors ("Sub-processor Lists"). Customer may receive notifications of new Sub-processors by emailing to subprocessor+subscribe@redguava.com.au to 'Subscribe', and if a Customer contact subscribes, Red Guava shall provide the subscriber with

notification of new Sub-processor(s) before authorising such new Sub-processor(s) to Process Customer Data in connection with the provision of the applicable Services. Customer hereby agrees that the aforementioned means of notification shall discharge Red Guava's notification provisions under Clause 9 of Exhibit B.

4.3. **Objection Right for New Sub-processors.** Customer may reasonably object to Red Guava's use of a new Sub-processor (e.g., if making Customer Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Customer Data) by notifying Red Guava promptly via email to dpa@redguava.com.au within ten (10) business days after receipt of Red Guava's notice in accordance with the mechanism set out in Section 4.2. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Red Guava will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Red Guava is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Agreement with respect only to those Services which cannot be provided by Red Guava without the use of the objected-to new Sub-processor by providing written notice to Red Guava. Red Guava will refund Customer any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

4.4. **Liability.** Red Guava shall be liable for the acts and omissions of its Sub-processors to the same extent Red Guava would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

5. Security

5.1. **Controls for the Protection of Customer Data.** Red Guava shall maintain appropriate technical and organisational measures for protection of the security (including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security Practices Datasheet. Red Guava regularly monitors compliance with these measures. Red Guava will not materially decrease the overall security of the Services during a subscription term.

5.2. **Third-Party Certifications and Audits.** Red Guava has access to the third-party certifications and audits set forth in the Security Practices Datasheet. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Red Guava shall make available to Customer (or Customer's independent, third-party auditor) information regarding the Red Guava's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Security Practices Datasheet. Customer may contact Red Guava via email to dpa@cliniko.com to request an on-site audit of Red Guava's procedures relevant to the protection of Customer Data, but only to

the extent required under applicable Data Protection Law. Customer shall reimburse Red Guava for any time expended for any such on-site audit at Red Guava's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Red Guava shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Red Guava. Customer shall promptly notify Red Guava with information regarding any non-compliance discovered during the course of an audit, and Red Guava shall use commercially reasonable efforts to address any confirmed non-compliance.

6. Personal data incident management and notification, DPIAs and prior consultation

Red Guava maintains security incident management policies and procedures specified in the Security Practices Datasheet. Red Guava shall notify Customer without undue delay of any breach relating to Customer Data (within the meaning of applicable Data Protection Law) of which Red Guava becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under applicable Data Protection Law or which Red Guava is required to notify to Customer under applicable Data Protection Law (a **"Customer Data Incident"**). Red Guava shall provide commercially reasonable cooperation and assistance in identifying the cause of such Customer Data Incident and take commercially reasonable steps to remediate the cause to the extent the remediation is within Red Guava's control. Except as required by applicable Data Protection Law, the obligations herein shall not apply to incidents that are caused by Customer, Authorised Users and/or any Non-Red Guava Products.

Upon Customer's request, Red Guava shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Red Guava. Red Guava shall provide reasonable assistance to Customer in the cooperation or prior consultation with a Supervisory Authority, to the extent required under Data Protection Laws.

7. Return and deletion of personal data

Upon termination of the Services for which Red Guava is Processing Customer Data, Red Guava shall, upon Customer's request, and subject to the limitations described in the Agreement and the Security Practices Datasheet, return all Customer Data in Red Guava's possession to Customer or securely destroy such Customer Data and demonstrate to the satisfaction of Customer that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Customer Data.

8. Controller Affiliates

8.1. **Contractual Relationship.** The parties acknowledge and agree that, by accepting the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between Red Guava and each such Controller Affiliate subject to the provisions of the Agreement and this Section 8 and Section 9. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Controller Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Customer.

8.2. **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Red Guava under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

8.3. **Rights of Controller Affiliates.** If a Controller Affiliate becomes a party to the DPA with Red Guava, it shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

8.3.1. Except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against Red Guava directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together (as set forth, for example, in Section 8.3.2, below).

8.3.2. The parties agree that the Customer that is the contracting party to the Agreement shall, if carrying out an on-site audit of the Red Guava procedures relevant to the protection of Customer Data, take all reasonable measures to limit any impact on Red Guava by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Controller Affiliates in one single audit.

9. Limitation of Liability

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Controller Affiliates and Red Guava, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means

the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Red Guava and its Affiliates' total liability for all claims from the Customer and all of its Controller Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Controller Affiliate that is a contractual party to any such DPA.

10. Legal Effect

This DPA shall only become legally binding between Customer and Red Guava when Customer accepts the Agreement. If Customer has previously executed an EU Data Processing Addendum with Red Guava, this DPA supersedes and replaces such prior EU Data Processing Addendum.

11. Governing Law

This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of Ireland.

List of Exhibits

Exhibit A: Description of Processing Activities
Exhibit B: Standard Contractual Clauses

EXHIBIT A
Description of Processing Activities

Nature and purpose of the processing

To allow Red Guava to deliver the Services to Customer, together with the Purpose.

Nature and purpose of sub-processing

To allow Red Guava to outsource certain elements of the Services, together with the Purpose.

Duration of processing

For the term of the Agreement.

Data subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer and which may include, but is not limited to, Personal Data relating to the following categories of Data Subject:

- Authorised Users;
- employees of Customer;
- consultants of Customer;
- contractors of Customer;
- agents of Customer; and/or
- third parties with whom the Customer conducts business, or about whom the Customer obtains information in the course of and for the purpose of conducting business.

Categories of data

The Personal Data transferred concern the following categories of data:

Any Personal Data comprised in Customer Data, as defined in the Agreement.

Special categories of data

Customer may submit Personal Data to Red Guava through the Services, the extent of which is determined and controlled by Customer in compliance with applicable Data Protection Law and which may concern the following special categories of data, if any:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;

- genetic or biometric data;
- health; and
- data concerning a person's sex life or sexual orientation.

Processing operations

The Personal Data transferred will be Processed in accordance with the Agreement and any Order Form and may be subject to the following Processing activities:

- storage and other Processing necessary to provide, maintain, and update the Services provided to Customer;
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Agreement, as compelled by law.

Frequency of the transfer

The transfer shall be continuous and for the duration the Services are provided to Customer.

EXHIBIT B
Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(e) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the

data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's

sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(a) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(b) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory

authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(a) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(b) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(c) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(d) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions,

pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and

will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of the Republic of Ireland.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Customer and Controller Affiliates

Data importer(s): Red Guava and its Affiliates

B. DESCRIPTION OF TRANSFER

See Exhibit A.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

…….

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See the Security Practices Datasheet.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors: see the Sub-processor Lists.