DATA PROCESSING GENERAL TERMS AND CONDITIONS

This Data Processing General Terms and Conditions ("DPA") forms a part of the Ecolab3D Program General Terms and Conditions ("General Terms and Conditions") and is entered into by and between Ecolab Inc. or one or more of its Affiliates and Customer (each a "Party" and collectively the "Parties"). The terms used in this DPA shall have the meanings set forth herein. Terms not otherwise defined herein shall have the meaning given to them in the General Terms and Conditions, unless such term has a specific meaning under Data Protection Law (as defined below), in which case the definition under Data Protection Law shall control. Except as modified herein, the terms of the General Terms and Conditions shall remain in full force and effect.

1. Definitions. In this DPA, the following terms shall have the meanings set out below and cognate terms under Data Protection Law shall be construed accordingly:

1.1. "**Controller**" shall have the meaning ascribed to it by Data Protection Law or, if there is no such definition in Data Protection Law, it means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Information.

1.2. "**Data Protection Law**" means applicable state and international comprehensive data protection laws, including, but not limited to (a) the European Union ("EU") General Data Protection Regulation ("GDPR"), European Economic Area ("EEA") laws, and the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the United Kingdom Data Protection Act 2018 (collectively "UK Data Protection Law"); (b) the California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq. ("CCPA"), and similar or other state data protection laws; (c) the Brazilian General Law on the Protection of Personal Data ("LGPD"); and (d) other applicable, comprehensive data protection laws with respect to any Personal Information processed under the General Terms and Conditions.

1.3. "**Data Subject**" means any identified or identifiable natural person as defined by Data Protection Law.

1.4. "**Personal Information**" means any personal information, as defined by the applicable Data Protection Law (also known as Personal Data or Personally Identifiable Information ("PII")) and including any sensitive or special categories of data) that is processed under or in connection with the General Terms and Conditions.

1.5. "**Process**" (including "process," "processing," and associated terms) means any operation or set of operations which is performed upon Personal Information.

1.6. "**Processor**" shall have the meaning ascribed to it by Data Protection Law or, if there is no such definition in Data Protection Law, it means a natural or legal person, public authority, agency or other body which processes Personal Information on behalf of the Controller.

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

1.8. "**Subprocessor**" means any person (including any third party but excluding personnel of Ecolab) appointed by or on behalf of Ecolab to process Personal Information in connection with the General Terms and Conditions.

1.9. The other capitalized and non-capitalized terms used in the DPA shall have the same meaning as in Data Protection Law, and their cognate terms shall be construed accordingly.

2. Roles of the Parties

2.1. The Parties agree that, for the purpose of Data Protection Law, Customer is the Controller and Ecolab is the Processor in relation to the processing of Personal Information and that such terms will have the meanings accorded to them pursuant to Data Protection Law.

2.2. Where Data Protection Law does not specifically utilize the terms Controller and Processor, the Parties shall be defined by the roles aligning with the cognate terms for Controller and Processor under the particular, applicable Data Protection Law.

3. Mutual Assurance of Compliance

3.1. Each Party acknowledges and confirms that it will comply with all applicable requirements of Data Protection Law and the terms of this DPA in relation to its processing of Personal Information.

3.2. Customer and Ecolab shall be separately responsible for conforming with such statutory data protection provisions as are applicable to each of them, and nothing in the DPA shall relieve a Party of its own statutory obligations.

4. Obligations of Ecolab

4.1. Ecolab shall:

4.1.1 retain, use, disclose, transfer or otherwise process the Personal Information only for the specified purpose of performance under the General Terms and Conditions as set out in Section 8 below;

4.1.2. process Personal Information only on documented instructions from Customer (as reflected in the General Terms and Conditions or other written or verbal communication);

4.1.3. not sell or "share" Personal Information, as those terms are defined by specific Data Protection Law (e.g. CCPA), including for cross context or targeted advertising (any limitation on "sharing" shall not apply to Ecolab's use of Subprocessor or other third parties for data processing where necessary to fulfill its obligations under the Program and Terms);

4.1.4. not retain, use, or disclose Customer's Personal Information (i) for any purpose other than the business purposes specified in the General Terms and Conditions (including retaining, using, or disclosing the Customer Personal Information for a commercial purpose other than the business purpose specified in the Program) or as otherwise permitted by applicable Data Protection Laws, or (ii) outside of the direct business relationship between Customer and Ecolab;

4.1.5 not combine Customer Personal Information regarding an individual that Ecolab receives from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another person, or collects from Ecolab's own interaction with the individual, provided that Ecolab may combine Customer's Personal Information to perform any Business Purpose as defined and permitted under applicable Data Protection Law;

4.1.6. ensure that persons authorized to process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

4.1.7. review and implement updates or binding regulatory guidance with respect to new Data Protection Law that are applicable to the General Terms and Conditions;

4.1.8. make available to Customer all information necessary to demonstrate Ecolab's compliance with its obligations under the General Terms and Conditions. Customer may, upon reasonable written notice to Ecolab, take reasonable and appropriate steps to stop and remediate any unauthorized use of personal information by Ecolab; and

4.1.9. promptly, and without undue delay, notify Customer if Ecolab determines that it can no longer meet its obligations under applicable Data Protection Laws.

4.2. The degree to which Ecolab directly receives a Data Subject request concerning a Customer's Data Subject, Ecolab shall notify Customer of such request. Ecolab shall forward such request to Customer and shall not respond to the Data Subject unless required by law. Upon Customer's reasonable written request, and the degree to which Customer is unable to fulfill a request without the assistance of Ecolab through available self-service or other options, Ecolab shall provide Customer with reasonable cooperation and assistance to enable a response to Data Subject's request.

4.3. If Ecolab receives a legally binding request or inquiry from a public authority or regulator for disclosure of Personal Information, it shall inform Customer of such request, unless prohibited by law. Ecolab agrees to provide Customer with reasonable assistance regarding such request, taking into account the nature of the processing and information available to Ecolab, including assisting Customer in challenging such request and leveraging any available appeals process.

4.4. As related to its processing of Personal Information, Ecolab shall notify Customer of any other requests or complaints regarding processing under the Program or Terms, including, but not limited to a) any requests or complaints received from Customer's employees or affiliates; or b) any request for disclosure of Personal Information not already defined herein that is related to the Program.

4.5. Ecolab shall provide reasonable assistance where Customer is required under applicable Data Protection Law to carry out assessments of the impact of the General Terms and Conditions or Program on the protection of Personal Information. In addition, Ecolab shall provide reasonable assistance where Customer is required under applicable Data Protection Law, to consult with a regulator regarding matters related to the processing of Personal Information under the General Terms and Conditions.

4.6. Customer consents to Ecolab engaging Subprocessors to process Personal Information for the purpose of performance under the General Terms and Conditions. Where Ecolab engages a Subprocessor for carrying out specific Personal Information processing activities as a part of performance under the General Terms and Conditions, Ecolab shall require legally compliant and industry standard data protection obligations based on the services provided and Personal Information processed by Subprocessor. A

current list of Ecolab's Subprocessors engaged in Processing of Personal Information on behalf of Customer are provided in Annex II. Ecolab will provide 30 days' notice to Customer prior to engaging a new Subprocessor. If Customer does not object within 30 days to the new Subprocessor, Customer is deemed to have approved Ecolab's engagement of the same.

5. Obligations of Customer

5.1. Customer shall inform Ecolab without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the processing of Personal Information detected during the course of such processing. Customer shall have sole responsibility for the accuracy, quality, and legality of personal information processed hereunder and the means by which Customer or any relevant Affiliate of Customer collects, stores, processes and transmits such personal information.

5.2. Where required by Data Protection Law, Customer is solely responsible for fulfilling its own notification duties towards Data Subjects, regulators, or other authorities.

5.3. If Customer receives any complaint, notice, or communication from a regulatory authority which relates to Ecolab's: (i) processing of the Personal Information; or (ii) potential failure to comply with Data Protection Law, Customer shall, to the extent permitted by law, promptly forward the complaint, notice, or communication to Ecolab and, where it relates to processing of Personal Information pursuant to this DPA, provide Ecolab with reasonable cooperation and assistance for responding to such complaint, notice, or communication.

5.4 Customer represents and warrants that Customer Data will not include any information deemed to be sensitive under any law or regulation (including any Data Protection Laws), including but not limited to health information, financial account numbers, any information of the type enumerated in Article 9 of the GDPR, or other similarly sensitive Personal Information. Customer assumes all risk arising from use of any such sensitive information with Program, including the risk of inadvertent disclosure or unauthorized access or use thereto.

6. Security

6.1. Taking into account industry standards, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Ecolab shall in relation to the Personal Information implement commercially reasonable technical and organizational measures specified in Annex I designed to ensure a level of security appropriate to that risk. In assessing the appropriate level of security, Ecolab shall take account of the risks that are presented by processing, in particular from a Security Incident. The technical and organizational measure applicable to a particular Program are available upon request, pursuant to the security measures described in the General Terms and Conditions and/or the Program.

6.2. If Ecolab learns of a Security Incident related to Personal Information processed under this DPA and/or the General Terms and Conditions, it shall give notification to Customer within a reasonable time. In the event of a Security Incident discovered on Ecolab-controlled systems, Ecolab will (i) investigate the Security Incident, (ii) provide Customer with information about the Security Incident (including, where possible, the nature of the Security Incident, Personal Information impacted by the Security Incident, and contact information of an individual at Ecolab from whom additional can be obtained), and (iii) take reasonable steps to mitigate the effects of, and to minimize any damage resulting from, the Security Incident.

6.3. If either Party learns of any inadvertent data disclosure or data breach concerning the other Party's data or systems, that Party shall give prompt notification to the other Party, and the Parties shall cooperatively establish a data breach notification and remediation plan, in compliance with Applicable Laws, with the responsibility for such notification and remediation plan being borne according to the Parties' respective, proportionate responsibility for the disclosure or breach and respective obligations under Applicable Laws.

6.4. Ecolab's liability for any Security Incident or any inadvertent data disclosure or data breach shall be subject to the provisions of Sections 4, 12, 13, and 14 of the General Terms and Conditions.

7. International Transfer of Personal Information and the Standard Contractual Clauses

7.1. If, as a part of the General Terms and Conditions, Ecolab or its Subprocessor(s) will process Personal Information originating from the European Economic Area in a country that has not been found to provide an adequate level of protection under applicable Data Protection Law, the Parties agree to enter into the EU Standard Contractual Clauses ("EU SCCs") and the United Kingdom Standard Contractual Clauses ("UK SCCs" and collectively with the EU SCCs, the "SCCs") as described in this section.

7.2. To facilitate transfer to third countries of Personal Information from the EU, Switzerland, or other EEA countries recognizing the sufficiency of the EU SCCs, the Parties agree to enter into the EU SCCs, as implemented by Commission Implementing Decision (EU) 2021/914 and as such EU SCCs may be revised or replaced from time to time. The Parties shall utilize Module 2 of the EU SCCs for controller-to-processor transfers. Customer, as Data Exporter, and Ecolab, as Data Importer, hereby

enter into, as of the Effective Date, the EU SCCs Module 2, which are incorporated by this reference and constitute an integral part of this DPA. The Parties are deemed to have accepted and executed the EU SCCs in their entirety, including the appendices. With regard to the EU SCCs, the Parties agree as follows:

7.2.1. Clause 7, "Docking Clause," shall not apply;

7.2.2. Clause 9, Option 2 shall apply and the "time period" shall be thirty (30) days;

7.2.3. Neither Party has engaged an independent dispute resolution body as described in Clause 11, and, as such, the optional provision shall not apply;

7.2.4. The EU Member State applicable for Option 1 of Clause 17 shall be (1) Germany or (2) the EU Member State in which a dispute between the Parties arises, or the EU Member State where a Data Subject brings a particular action;

7.2.5. The EU Member State applicable for Clause 18 shall be (1) Germany or (2) the EU Member State in which a dispute between the Parties arises, or the EU Member State where a Data Subject brings a particular action;

7.2.6. *Annex I* of the EU SCCs shall be deemed completed with the relevant sections of Section 8 of this DPA;

7.2.7. *Annex II* of the EU SCCs shall be deemed completed with the relevant sections of Annex I to this DPA; and

7.2.8. *Annex III* of the EU SCCs shall be deemed completed with the relevant sections of Annex II to this DPA.

7.3. To facilitate transfer of Personal Information from the UK to third countries, the Parties agree to enter into the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as issued by the UK's Information Commissioner's Officer ("ICO") under S119A(1) Data Protection Act 2018 (herein referred to as the "UK SCCs"). Customer, as Data Exporter, and Ecolab, as Data Importer, hereby enter into, as of the Effective Date, the UK SCCs, which are incorporated by this reference and constitute an integral part of this DPA. The Parties are deemed to have accepted and executed the UK SCCs in their entirety, including the appendices, with the relevant UK SCC tables deemed completed with the relevant information contained in Section 8 below and the Annexes to this DPA.

7.4. With regard to all international transfers of Personal Information, including, but not limited to the herein referenced SCCs:

7.4.1. At such time as the EU Commission, ICO, an EU Supervisory Authority, or other applicable regulator modifies any of the SCCs or implements new SCCs, such SCCs shall apply upon their effective date. The Parties agree that the references provided herein may be modified to include the new SCCs upon notice by either Party, without the need for subsequent DPA, unless otherwise required by law;

7.4.2. At such time as a country with applicable Data Protection Law established standard contractual clauses or similar documents that must be executed between the Parties, such clauses shall apply on their effective date. The Parties agree that this DPA may be modified to include the new standard contractual clauses upon notice to either Party, without the need for subsequent General Terms and Conditions, unless otherwise required by law; and

7.4.3. For Data Protection Law similar to GDPR requiring general terms and conditions for international transfer, but without required standard contractual clauses (e.g. Brazil, South Africa), the Parties agree that this DPA shall provide the required protection and general terms and conditions under said Data Protection Law.

8. Description of Processing

8.1. The categories of Data Subjects whose Personal Information is processed shall include the following, unless specifically defined in the Program or Terms: staff (e.g. employees, contractors) of Customer.

8.2. The categories of Personal Information processed shall include the following, unless specifically defined in the Program or Terms: basic contact information (e.g. business email, phone, and address).

8.3. No Personal Information classified as "sensitive" or "special" under Data Protection Law shall be processed unless specifically defined in a Program or Terms.

8.4. Personal Information shall be processed and transferred on a continuous basis for the Term of the Program and Terms.

8.5. The nature of the Personal Information processing shall be defined in the Program and Terms.

8.6. The purpose(s) of the Personal Information processing and transfer shall be to provide services as described in the General Terms and Conditions and Program.

8.7. The period for which the Personal Information will be retained shall be the Term of the Program or for a shorter period as instructed by Customer.

8.8. For transfers to Subprocessors, the subject matter and duration of the processing is as outlined above within this Section 8. The nature of the specific subprocessing services is as further described in the Subprocessor List provided by Ecolab.

9. Term and termination

9.1. This DPA shall have the same term as the General Terms and Conditions.

9.2. Without prejudice to any other termination rights that a Party may have under this DPA and/or applicable law, each Party may terminate its participation in this DPA if it finds the other Party is not in compliance with the terms of this DPA, provided that the Party found not in compliance shall have opportunity to cure consistent with the General Terms and Conditions.

9.3. Upon termination, each Party shall be entitled to keep Personal Information only as may be necessary to fulfill any ongoing purposes or requirements of the General Terms and Conditions. Any Personal Information no longer needed to fulfill ongoing purposes or requirements defined in the General Terms and Conditions may be deleted by Ecolab within 90 days of Termination, with appropriate exception for deletion where backup copies of Personal Information are logically deleted on a longer schedule, or if retention for a longer schedule is required or permitted by Applicable Laws.

10. Miscellaneous

10.1. This DPA inures to the benefit of the Parties only and no third party shall have any rights hereunder, except as otherwise stated herein.

10.2. A determination that any provision of the DPA is invalid or unenforceable shall not affect the other provisions of the DPA. In such case the invalid or unenforceable provision shall automatically be replaced by a valid and enforceable provision that comes closest to the purpose of the original provision. The same shall apply if the DPA contains an unintended gap.

10.3 To the extent there is any conflict between the Agreement, this DPA, and/or the SCCs, the various agreements will control in the following order of preference: (i) the SCCs, (ii) this DPA, (iii) the General Terms and Conditions.

ANNEX I - TECHNICAL AND ORGANIZATIONAL MEASURES

Description of the technical and organizational measures implemented by Ecolab 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:

(A) Control of physical access to premises	Technical and organizational measures to control physical access to premises and facilities, particularly to identify permitted personnel at entry: ☒ Locked doors on all entrances / exits ☒ Presence of security personnel ☒ Access control systems ☒ CCTV systems ☒ Burglar alarm systems
(B) Control of access to IT systems	Technical and organizational security measures designed to ensure that users with access to the relevant IT systems are identified and authenticated: ☒ IT security systems requiring individual users to log in using unique user names ☒ IT security systems requiring the use of strong / complex passwords ☒ IT security systems requiring the use of multi-factor authentication ☒ Additional system log-in requirements for particular applications ☒ Mandatory password changes at fixed intervals ☒ Encryption applied to personal data 'in transit' ☒ Encryption applied to personal data 'at rest' ☒ Automatic locking of IT terminals and devices after periods of non-use, with passwords required to 'wake' the terminal or device ☒ Password databases are subject to strong encryption / hashing ☒ Regular audits of security procedures ☒ Training for employees regarding access to IT systems
(C) Control of access to personal data	Technical and organizational security measures designed to ensure that users with access to the relevant personal data are identified and authenticated: ☒ 'Read' rights for systems containing personal data restricted to specified personnel roles ☒ 'Edit' rights for systems containing personal data restricted to specified personnel roles or profiles ☒ Logging of attempts to access systems containing personal data ☒ Encryption on drives and media containing personal data ☒ Training for employees regarding access to personal data

(D) Control of disclosure of personal data	Technical and organizational measures to securely transfer, transmit and communicate or store data on data media and for subsequent checking: ☒ Restrictions on transfer rights for systems containing personal data ☒ Secure data networks ☒ Encryption for systems used to send personal data ☒ SSL encryption for all internet access portals ☒ Protection of data storage media and containers during physical transport ☒ Training for employees regarding transfers of personal data
(E) Control of input mechanisms	Technical and organizational security measures to permit the recording and later analysis of information about when input to data systems (e.g., editing, adding, deleting, etc.) occurred and who was responsible for such input: ☒ Logging of all input actions in systems containing personal data ☒ 'Edit' rights for systems containing personal data restricted to specified personnel roles or profiles ☒ Binding agreements in writing or other obligations of confidentiality with employees who process personal data ☒ Regular reviews of compliance with the relevant agreements ☒ Training for employees regarding editing of personal data
(F) Control of workflows between controllers and processors	Technical and organizational measures to segregate the responsibilities between controllers and processors processing the relevant personal data: ☒ Binding agreements in writing governing the appointment and responsibilities of processors with access to the relevant personal data ☒ Binding agreements in writing governing the allocation of data protection compliance responsibilities between all controllers with access to the relevant personal data ☒ Regular reviews of compliance with the relevant agreements ☒ Training for employees regarding processing of personal data
(G) Control mechanisms to ensure availability of the relevant personal data	Technical and organizational measures to ensure the physical and electronic availability and accessibility of the relevant personal data: ☒ Documented disaster recovery procedures ☒ Secure backup procedures in place, with full backups run regularly ☒ Backup facilities and locations ☒ Uninterruptible power supplies at backup facilities ☒ Physical security of backup facilities ☒ Security alarm systems at backup facilities ☒ Electronic security of backup facilities ☒ Environmental controls at backup facilities ☒ Fire protection at backup facilities ☒ Deidentification or deletion of personal data that are no longer required for lawful processing purposes ☒ Training for employees regarding backups and disaster recovery

(H)	**Control mechanisms to ensure separation of the relevant personal data from other data**	Technical and organizational measures to ensure that the relevant personal data are stored and processed separately from other data: ☒ Logical separation of live or production data from backup data and development or test data ☒ Separation of personnel processing the relevant personal data from other personnel ☒ Training for employees regarding data separation

ANNEX II – LIST OF SUBPROCESSORS

The controller has authorized the use of the Subprocessors found in its Subprocessor List available below:

Subprocessor	Subprocessor Address
Microsoft	1 Microsoft Way, Redmond, WA 98052
Cisco AppDynamics	500 Terry A Francois Blvd, 3rd fl San Francisco, CA 94158
Sales Force	415 Mission Street, 3rd Floor, San Francisco, CA
LinkedIn Sales Navigator	1000 W. Maude Ave, Sunnyvale, CA 94085
Microsoft Dynamics CRM	1 Microsoft Way, Redmond, WA 98052
Soprano Design Pty	Level 15, 132 Arthur St North Sydney NSW 2060 Australia
ServiceNow	2225 Lawson Lane, Santa Clara, CA 95054 Hoekenroder 3, Amsterdam Zuidoost, North Holland 1102 BR 80 Robinson Road, #02-00, Singapore 068898
FiveTran	1221 Broadway Street, Floor 20, San Francisco, CA