

## Insycle Data Processing Agreement

This Insycle Data Processing Agreement reflects the agreement between Insycle Inc. (“Insycle”, “we”, “us”) and you (“Customer” or “you”) with respect to the Processing of Personal Data by Insycle on your behalf in connection with your use of the Insycle Service pursuant to the Insycle [Terms of Service](#) between you and us (the “Agreement”). Capitalized terms not otherwise defined herein will have the meaning as set forth in the Agreement.

The term “DPA” as used herein includes:

1. This **Insycle Data Processing Agreement**.
2. **Annex I** – Details of the Processing, attached hereto.
3. **Annex II** - Technical and Organizational Security Measures, attached hereto.
4. **Annex III** – List of Sub-Processors, attached hereto.
5. The [Standard Contractual Clauses](#), to the extent applicable, in which case the relevant Module shall be deemed incorporated herein by this reference, as follows:
  - a. To the extent Customer transfers Personal Data to Insycle as a Controller of such Personal Data (where Insycle is a Processor), **Module 2** of the Standard Contractual Clauses shall apply with respect to Insycle’s Processing of such Personal Data and is hereby incorporated.
  - b. To the extent Customer transfers Personal Data to Insycle as a Processor or Sub-Processor of such Personal Data (where Insycle is a Sub-Processor), **Module 3** of the Standard Contractual Clauses shall apply with respect to Insycle’s Processing of such Personal Data and is hereby incorporated.

This DPA is supplemental to, and forms part of, the Agreement upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order, or an executed amendment to the Agreement.

The term of this DPA will commence upon execution hereof and will expire upon expiration or earlier termination of the Agreement.

This DPA was last updated on November 24, 2021. You can find archived versions of the DPA [here](#).

## 1. Definitions

**"California Personal Information"** means Personal Data that is subject to the protection of the CCPA.

**"CCPA"** means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

**"Consumer", "Business", "Sell" and "Service Provider"** will have the meanings given to them in the CCPA.

**"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

**"Customer"** means the party executing this DPA as Customer below.

**"Customer Data"** means Personal Data submitted or provided by or for Customer, or at Customer's direction, to Insycle in connection with Customer's use of the Insycle Service, and to which Data Protection Laws apply.

**"Data Protection Laws"** means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws and the CCPA; in each case as amended, repealed, consolidated or replaced from time to time.

**"Data Subject"** means the individual to whom Personal Data relates.

**"Europe"** means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

**"European Data"** means Personal Data that is subject to the protection of European Data Protection Laws.

**"European Data Protection Laws"** means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

**“Instructions”** means the written, documented instructions issued by Customer to Insycle, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

**“Personal Data”** means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

**“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Insycle Service. “Personal Data Breach” will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

**“Privacy Shield”** means the EU-U.S. and Swiss-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to its Decision of July 12, 2016 and by the Swiss Federal Council on January 11, 2017 respectively; as may be amended, superseded or replaced.

**“Privacy Shield Principles”** means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of July 12, 2016; as may be amended, superseded or replaced.

**“Processing”** means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

**“Processor”** means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

**“Standard Contractual Clauses”** means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR, as may be amended, superseded, or replaced.

**“Sub-Processor”** means any Processor engaged by us or our Affiliates to Process Customer Data on our behalf in fulfilling our obligations with respect to the provision of the

Insycle Service under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any Insycle employee or consultant.

“**Transparency Report**” is the publicly available report including information regarding requests made by government agencies or law enforcement officials to obtain Personal Data from Insycle and that is located at <https://www.insycle.com/transparencyreport> or at such other URL as Insycle may provide from time to time.

## 2. Customer Responsibilities

a. *Compliance with Laws.* Within the scope of the Agreement and with respect to your use of the Services, you will be responsible for complying with all requirements that apply to you under applicable Data Protection Laws with respect to your Processing of Customer Data and the Instructions you issue to us.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which you acquired the Customer Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Customer Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Customer Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any content created, sent or managed through the Insycle Service, including those relating to obtaining consents (where required). You will inform us without undue delay if you are not able to comply with your responsibilities under this ‘Compliance with Laws’ section or applicable Data Protection Laws.

b. *Customer Instructions.* The parties agree that the Agreement (including this DPA), together with your use of the Insycle Service in accordance with the Agreement, constitute your complete Instructions to us in relation to the Processing of Customer Data. Any additional Instructions provided during the subscription term must be consistent with the Agreement, the nature and intended use of the Insycle Service, and the lawful use of the Insycle Service. Additional Instructions outside the scope of this DPA require prior written agreement between the parties.

c. *Security.* You are responsible for independently determining whether the data security provided for in the Insycle Service adequately meets your obligations under applicable Data Protection Laws. You are also responsible for your secure use of the

Insycle Service, including protecting the security of Customer Data in transit to and from the Insycle Service (including to securely backup or encrypt any such Customer Data).

### 3. Insycle Obligations

a. *Compliance with Instructions.* We will only Process Customer Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

b. *Conflict of Laws.* If we become aware that we cannot Process Customer Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Customer Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Insycle Service until such time as you issue new lawful Instructions with regard to the Processing.

c. *Security.* We will implement and maintain appropriate technical and organizational measures designed to protect Customer Data from Personal Data Breaches, as described under Annex II to this DPA ("**Security Measures**"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

d. *Confidentiality.* We will ensure that any personnel whom we authorize to Process Customer Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Customer Data.

e. *Personal Data Breaches.* We will notify you without undue delay after we become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

f. *Deletion or Return of Personal Data.* Other than to the extent required to comply with Data Protection Law, following termination or expiry of the Agreement, Insycle will delete all Customer Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Customer Data for technical or other reasons, Processor will apply measures to ensure that Customer Data is blocked from any further Processing.

Customer shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Customer Data after the termination or expiration of the Agreement shall be borne by Customer. This term shall apply except where we are required by applicable law to retain some or all of the Customer Data, or where we have archived Customer Data on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with our deletion practices. You may request the deletion of your Insycle account after expiration or termination of your subscription. You may also cancel your account in accordance with the 'Termination' section of the Agreement and request permanent deletion.

#### **4. Data Subject Requests**

The Insycle Service provides you with a number of controls that you can use to retrieve, correct, delete or restrict Customer Data, which you can use to assist you in connection with your obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("**Data Subject Requests**").

To the extent that you are unable to independently address a Data Subject Request through the Insycle Service, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Customer Data under the Agreement. You shall reimburse us for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Customer Data under the Agreement is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Customer Data.

#### **5. Sub-Processors**

You agree that we may engage Sub-Processors to Process Customer Data on your behalf. We have currently appointed, as Sub-Processors, the third parties listed in Annex III to this DPA. We will notify you if we add or replace any Sub-Processors listed in Annex III at least thirty (30) days prior to any such changes via email to the email address(es) on record in Insycle's account information for Customer.

Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain

responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of our obligations under this DPA.

## 6. Data Transfers

You acknowledge and agree that we may access and Process Customer Data on a global basis as necessary to provide the Insycle Service in accordance with the Agreement, and in particular that Personal Data may be transferred to and Processed by Insycle, Inc. in the United States and to other jurisdictions where Insycle Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

## 7. Additional Provisions for European Data

a. *Scope.* This 'Additional Provisions for European Data' section shall apply only with respect to European Data.

b. *Transfer Mechanisms for Data Transfers.*

(A) Insycle shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

(B) You acknowledge that in connection with the performance of the Insycle Services, Insycle Inc. is a recipient of European Data in the United States. The parties acknowledge and agree the following:

(a) Standard Contractual Clauses: The parties agree to abide by and process European Data in compliance with the Standard Contractual Clauses, subject to the provisions of this Section 7 of the DPA.

(b) Privacy Shield: Although Insycle, Inc. does not rely on the EU-US Privacy Shield as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for as long as Insycle is self-certified to the Privacy

Shield, Insycle will process European Data in compliance with the Privacy Shield Principles and let you know if it is unable to comply with this requirement.

(C) The parties agree that for the purposes of the Standard Contractual Clauses, (i) Insycle Inc. will be the "data importer" and Customer will be the "data exporter"; (ii) the Annexes of the Standard Contractual Clauses shall be populated with the relevant information set out in Annex I and Annex II of this DPA; (iii) where the Insycle contracting entity under the Agreement is not Insycle, Inc., such contracting entity (not Insycle, Inc.) will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses by Insycle, Inc., and you will direct any instructions, claims or enquiries in relation to the Standard Contractual Clauses to such contracting entity; and (iv) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

(D) To extent that and for so long as the Standard Contractual Clauses as implemented in accordance with this DPA cannot be relied on by the parties to lawfully transfer Personal Data in compliance with the UK GDPR, the applicable standard data protection clauses issued, adopted or permitted under the UK GDPR shall be incorporated by reference, and the annexes, appendices or tables of such clauses shall be deemed populated with the relevant information set out in Annex I and Annex II of this DPA.

(E) If for any reason Insycle cannot comply with its obligations under the Standard Contractual Clauses or is in breach of any warranties under the Standard Contractual Clauses, and you intend to suspend the transfer of European Data to Insycle or terminate the Standard Contractual Clauses, you agree to provide us with reasonable notice to enable us to cure such non-compliance and reasonably cooperate with us to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If we have not or cannot cure the non-compliance, you may suspend or terminate the affected part of the Insycle Service in accordance with the Agreement without liability to either party (but without prejudice to any fees you have incurred prior to such suspension or termination).

c. *Instructions.* If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay. For purposes of Clause 8.1 of the Standard Contractual Clauses, the parties agree that Section 2.b of this DPA contains the complete Instructions of Customer for Insycle's Processing of Customer Data.

d. *Certification of Deletion.* Customer agrees that the certification of deletion of Personal Data that is described in Clause 8.5 of the Standard Contractual Clauses shall be provided by Insycle to Customer only upon Customer's written request.

e. *Personal Data Breaches.* The parties agree that if a Sub-Processor suffers a Personal Data Breach affecting Customer Data, Insycle will use commercially reasonable



efforts to ensure that the Sub-Processor takes appropriate measures to address the breach, including measures to mitigate its adverse effects in accordance with Clause 8.6.(c) of the Standard Contractual Clauses.

f. *Sub-Processor Engagement.* Customer consents to Insycle's transfer of Personal Data to Sub-Processors as described in Section 5 of this DPA and agrees that this Customer consent satisfies the requirements of Clauses 9(a) and 9(b) of the Standard Contractual Clauses. For the avoidance of doubt, the above authorization constitutes Customer's general authorization for the engagement of Sub-Processors by Insycle by for purposes of Clause 9(a) of the Standard Contractual Clauses.

g. *Sub-Processor Objection.* Insycle will give you the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 30 days of notifying you in accordance with the 'Sub-Processors' section. If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Insycle Service in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination). The parties agree that by complying with this sub-section, Insycle fulfills its obligations under Clause 9(a) of the Standard Contractual Clauses.

h. *Sub-Processor Agreements.* For the purposes of Clause 9(c) of the Standard Contractual Clauses, you acknowledge that we may be restricted from disclosing Sub-Processor agreements, but we shall use reasonable efforts to require any Sub-Processor we appoint to disclose the Sub-Processor agreement to you and shall provide (on a confidential basis) all information we reasonably can.

i. *Data Protection Impact Assessments and Consultation with Supervisory Authorities.* To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws. You will reimburse us for the commercially reasonable costs arising from this assistance.

j. *Insycle Obligations in Case of Access by Public Authorities.* To the extent permitted by applicable laws, Insycle will inform Customer of any request it receives to disclose Personal Data if Customer subscribes to receive such notifications by using the mechanism set forth in the Transparency Report. Customer agrees that the mechanism set forth in the Transparency Report satisfies the requirements under Clause 15.1(c) of the

Standard Contractual Clauses. Insycle agrees to frequently update the Transparency Report.

k. *Demonstration of Compliance.* We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA and Clause 8.9 of the Standard Contractual Clauses. You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section. You acknowledge that the Insycle Service is hosted by our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001). At your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year unless you have reasonable grounds to suspect non-compliance with the DPA. You shall reimburse us for the commercially reasonable costs arising from our responses to your requests hereunder. Customer agrees that this Section 7(k) of the DPA satisfies Customer's rights under Clauses 8.9.(c) and 8.9.(d) of the Standard Contractual Clauses.

l. *Governing Law.* With respect to Clause 17 of the Standard Contractual Clauses, the Standard Contractual Clauses shall be governed by the law of the EU Member State in which the Customer is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

m. *Choice of Forum and Jurisdiction.* With respect to Clause 18 of the Standard Contractual Clauses: (a) any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of an EU Member State; (b) the Parties agree that those shall be the courts 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; and (d) the Parties agree to submit themselves to the jurisdiction of such courts.

n. *Conflict.* In the event of any conflict or inconsistency between (i) the body of this DPA (other than this Section 7), (ii) this Section 7 of the DPA, and (iii) the Standard Contractual Clauses, the order of precedence shall be: (i) the Standard Contractual Clauses, (ii) this Section 7 of the DPA, and (iii) the body of this DPA (other than this Section 7).

## **8. Additional Provisions for California Personal Information**

a. *Scope.* The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

b. *Roles of the Parties.* When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA, as such terms are defined in the CCPA.

c. *Responsibilities.* The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Insycle Service under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA, including as described in the Privacy Policy.

## 9. General Provisions

a. *Amendments.* Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, we reserve the right to make any updates and changes to this DPA from time to time. If you have an active subscription to the Insycle Service, we will let you know when we make updates, via email (if you have subscribed to receive email notifications).

b. *Conflicts; Severability.* In case of any conflict between the terms of the Agreement and the terms of this DPA, this DPA shall take precedence over the provisions of the Agreement. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

c. *Limitation of Liability.* Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the Agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA). For the avoidance of doubt, if Insycle Inc. is not a party to the Agreement, the 'Limitation of Liability' section of the Agreement will apply as between you and Insycle Inc., and in such respect any references to 'Insycle', 'we', 'us' or 'our' will include both Insycle Inc. and the Insycle entity that is a party to the Agreement. In no event shall either party's liability be limited with respect to any individual data subject's data protection rights under this DPA (including the Standard Contractual Clauses) or otherwise.

d. *Governing Law.* This DPA will be governed by and construed in accordance with the 'Choice of Law and Forum' section of the Agreement, unless otherwise required by Data Protection Laws.

e. *Assistance.* With respect to any assistance provided to you by Insycle, responses to requests from you hereunder, and/or other assistance provided by Insycle to you under this DPA or the Data Protection Laws, you agree to reimburse Insycle for the commercially reasonable costs arising from such assistance and response to requests.

## 10. Parties to this DPA

a. *Authorization.* The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself.

c. *Remedies.* The parties agree that the Customer entity that is the contracting party to the Agreement will solely exercise any right or seek any remedy it may have under this DPA on behalf of its Affiliates. The Customer entity that is the contracting entity is responsible for coordinating all Instructions, authorizations and communications with us under the DPA and will be entitled to make and receive any communications related to this DPA on behalf of its Affiliates.

d. *Other rights.* The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Affiliates in one single audit.

**IN WITNESS WHEREOF**, the Parties have caused their respective duly authorized representatives to execute this Data Processing Agreement.

Insycle Inc.

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Customer: \_\_\_\_\_

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## Annex I - Details of the Processing

### A. List of Parties

#### Data exporter(s):

The Customer, as defined in the Insycle Terms of Service (the "Agreement")

\*Name: \_\_\_\_\_

\*Address: \_\_\_\_\_

\*Contact person's name, position and contact details: \_\_\_\_\_

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Services under the Agreement.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

\*Role of Customer (please select one option):

- Controller (Module 2 – Controller to Processor)
- Processor (Module 3 - Processor to Sub-Processor)

*\*Items marked with an asterisk must be completed by Customer prior to signature.*

#### Data importer(s):

Name: Insycle Inc.

Address: 80 Leonard Street, New York, NY 10013

Contact person's name, position and contact details: \_\_\_\_\_

Email: \_\_\_\_\_; Phone Number: \_\_\_\_\_

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Insycle Services under the Agreement.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Role (controller/processor):

- Processor (Module 2 – Controller to Processor)
- Sub-Processor (Module 3 - Processor to Sub-Processor)

## B. Description of Transfer

### Categories of data subjects whose personal data is transferred

Customer's Contacts and other end users including Customer's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Customer's end users.

### Categories of personal data transferred

Contact Information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Insycle Service.

### Sensitive data transferred (if applicable)

The parties do not anticipate the transfer of sensitive data.

### The frequency of the transfer

Continuous

### Nature of the processing

The nature of Processing of Personal Data by Insycle is the provision of the services to the Customer that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order.

### Purpose(s) of the data transfer and further processing

Personal Data will be Processed for purposes of providing the services set out and otherwise agreed to in the Agreement and any applicable Order

### 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 Processed for the duration of the Agreement, subject to Section 3(f) of the DPA.

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

The subject matter, nature and duration of the processing is set forth in the Agreement and the DPA. See Annex III for additional information.

### C. Competent Supervisory Authority

The supervisory authority that shall act as competent supervisory authority is either (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; (ii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established; or (iii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. If a competent supervisory authority is not established as set forth above, the parties hereby select the Irish Data Protection Commission to the extent legally permissible.

In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).

## Annex II - Security Measures

Insycle currently observes the security practices described in this Annex II. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, Insycle may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

### **a) Access Control**

#### **i) Preventing Unauthorized Product Access**

**Outsourced processing:** Insycle hosts its Service with outsourced cloud infrastructure providers. Additionally, Insycle maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Insycle relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

**Physical and environmental security:** Insycle hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

**Authentication:** Insycle implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

**Authorization:** Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Insycle's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

**Application Programming Interface (API) access:** Public product APIs may be accessed using an API key or through OAuth authorization.

#### **ii) Preventing Unauthorized Product Use**

Insycle implements industry standard access controls and detection capabilities for the internal networks that support its products.



**Access controls:** Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

**Static code analysis:** Security reviews of code stored in Insycle's source code repositories is performed, checking for coding best practices and identifiable software flaws.

### iii) Limitations of Privilege & Authorization Requirements

**Product access:** A subset of Insycle's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

## b) Transmission Control

**In-transit:** Insycle makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Insycle products. Insycle's HTTPS implementation uses industry standard algorithms and certificates.

**At-rest:** Insycle stores user passwords following policies that follow industry standard practices for security. With effect 25 May 2018, Insycle has implemented technologies to ensure that stored data is encrypted at rest.

## c) Input Control

**Detection:** Insycle designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Insycle personnel, including security, operations, and support personnel, are responsive to known incidents.

**Response and tracking:** Insycle maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Insycle will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Insycle becomes aware of unlawful access to Customer data stored within its products, Insycle will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Insycle is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Insycle deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Insycle selects, which may include via email or telephone.

#### **d) Availability Control**

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

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.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Insycle's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Insycle operations in maintaining and updating the product applications and backend while limiting downtime.

## Annex III – Sub-Processors

Customer has authorised Insycle’s use of the following Sub-processors:

Name	Address	Contact Information	Description of Processing
Google, Inc.	1600 Amphitheatre Parkway Mountain View, California USA 94043	<a href="https://cloud.google.com/security/compliance">https://cloud.google.com/security/compliance</a>	Main hosting provider for the production application. Primary holder of application data.
Twilio, Inc.	375 Beale Street, Suite 300   San Francisco, CA USA 94105	<a href="https://www.twilio.com/trust">https://www.twilio.com/trust</a>	Sends application texts/SMS for customer configured alerts.
SendGrid, Inc.	1801 California Street, Suite 500, Denver, Colorado USA 80202	<a href="https://sendgrid.com/policies/security/">https://sendgrid.com/policies/security/</a>	Sends application emails for customer configured alerts.

If you would like to receive an email when we make updates to this Annex 3, click [here](#).