SHORTSTACK

DATA PROCESSING ADDENDUM

(January 2022)

This Data Processing Addendum ("DPA") forms part of the Pancake Laboratories Inc, DBA ShortStack.com ("ShortStack) Terms and Conditions (https://www.shortstack.com/terms-and-conditions/), ShortStack Privacy Policy (https://www.shortstack.com/privacy-policy/) and other written or electronic agreement by and between ShortStack and its affiliates (collectively, "Pancake Laboratories, Inc" referred to herein as "Pancake") and the undersigned customer of ShortStack ("Customer") for the purchase of online services ("Services") from Pancake (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.

HOW TO EXECUTE THIS DPA:

1. This DPA has been pre-signed on behalf of Pancake.

2. The Standard Contractual Clauses in Schedule 1 have been pre-signed by Pancake as the data importer.

3. To complete this DPA, Customer must
    a. Complete the information and sign on page 14;
    b. Complete the information as the data exporter on page 15; and
    c. Complete the information and sign as data exporter on page 32.

4. Send the completed and signed DPA to Pancake by email, indicating the email address associated with your ShortStack.com account, to contact@shortstacklab.com.

Upon receipt by Pancake of signed DPA from Customer via email, this DPA will become legally binding.

DATA PROCESSING TERMS

In the course of providing the Services to Customer pursuant to the Agreement, Pancake may Process Personal Data on behalf of Customer. Both Pancake and Customer agree to comply with the following provisions with respect to any Personal Data submitted by or for Customer to Pancake or collected and processed by or for Customer using Pancake Services.

In connection with the Service, the parties anticipate that Pancake may process outside of the European Economic Area ("EEA"), Switzerland, the United Kingdom, Canada, Australia and Brazil, Personal Data in respect of which the Customer or any member of the Customer Group may be a data controller under applicable Data Protection Laws and Regulations.

1. DEFINITIONS
    1.1. In this DPA, the following terms shall have meanings set below and cognate terms shall be constructed accordingly:

        1.1.1. "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.

        1.1.2. "Applicable Laws" means (a) European Union, the European Economic Area or member state, Switzerland, the United Kingdom, Canada, Australia, California and Brazil, laws with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to European Data Protection Laws and Regulations and non-European Data Protection Laws and Regulations; and (b) any other applicable law with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to any other Data Protection Laws and Regulations;

        1.1.3. "Customer Group" means Customer and any of Customer's Affiliate(s) which (a) is subject to European Data Protection Laws

and Regulations and Non-European Data Protection Laws and Regulations, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Pancake, is not a "Customer" as defined under the Agreement.

1.1.4. "Controller" means the entity which determines the purposes and means of the Processing of Personal Data or an entity defined as a "Business" under the CCPA.

1.1.5. "Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data."

1.1.6. "Data Protection Laws and Regulations" means all laws and regulations, including European Data Protection Laws and Non-European Data Protection Laws, and, to the extent applicable, the data protection or privacy laws of any other country applicable to the Processing of Personal Data under the Agreement.

1.1.7. "Data Subject" means the identified or identifiable person, or "Consumer" as defined under the CCPA, to whom Personal Data relates.

1.1.8. "EU GDPR" means the General Data Protection 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.

1.1.9. "European Data Protection Laws" means all data protection laws and regulations applicable to Europe, including (a) the EU GDPR; (b) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (c) applicable national implementations of (a) and (b); (d) the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 ("UK GDPR") and the UK Data Protection Act 2018 (together, "UK

DPA"); and (e) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance ("Swiss DPA").

1.1.10. "Non-European Data Protection Laws" means the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018; and the Privacy Act 1988 (Cth) of Australia, as amended ("Australian Privacy Law").

1.1.11. "Party" means either the Data Processor or Data Controller, and "Parties" means both the Data Processor and Data Controller.

1.1.12. "Personal Data" means any information about a natural person that is identified or identifiable to the natural person, either alone or in combination with other information, that Pancake will process or have access to as part of providing the Services, including any such information that is created by means of the Services and data defined as "Personal Information" under the CCPA.

1.1.13. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.1.14. "Processing" means any operation or set of operations which is performed upon Personal Data, including such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

1.1.15. "Processor" means the entity which Processes Personal Data on behalf of the Controller or an entity defined as a "Service Provider" under the CCPA.

1.1.16. “Sensitive Data” means (a) social security number, tax file number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number; (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of “special categories of data” under applicable Data Protection Laws and Regulations.

1.1.17. “Service Data” means any electronic data, communications or other materials, including Personal Data, which is collected, stored, transmitted or otherwise processed via Pancake Services, by, or on behalf of, Customer and Customer’s end-users.

1.1.18. “Standard Contractual Clauses” means (a) where the EU GDPR applies, the clauses attached hereto as Schedule 1 pursuant to the European Commission’s Implementing Decision (EU) 2021/91 of 4 June 2021decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data from controllers to processors established in third countries which do not ensure an adequate level of data protection (“EU SCCs”); and (b) where the UK GDPR applies, the standard data protection clauses for processors adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs"); in each case as may be amended, superseded or replaced from time to time.

1.1.19. “Subprocessor” means any Processor engaged by Pancake.

1.2. The terms, “Commission”, “Member State”, and “Supervisory Authority” shall have the same meaning as in the EU GDPR, and their cognate terms shall be construed accordingly.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data when using the Service provided by Pancake, Customer is the Controller, Pancake is the Processor and that Pancake will engage Subprocessors pursuant to the requirements set forth in Section 5 "Subprocessors" below.

2.2. Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. 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. Pancake's Processing of Personal Data. Pancake shall treat Personal Data as Confidential Information and shall Process Personal Data in a manner compliant with Data Protection Laws and Regulations and the requirements regarding the collection, use and retention of Personal Data of Data Subjects. Pancake will only process Personal Data to the extent necessary to perform the Services in accordance with the Agreement and in accordance with Customer's written instructions.

2.4. Prohibited data. Customer will not provide (or cause to be provided) any Sensitive Data to Pancake for processing under the Agreement, and Pancake will have no liability whatsoever for Sensitive Data, whether in connection with a Personal Data Breach or otherwise.

2.5. Details of the Processing. The subject-matter of Processing of Personal Data by Pancake is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 Appendix Annex I.B (Description of Transfer) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1. Data Subject Request. Pancake shall promptly notify Customer if Pancake receives a request from a Data Subject to exercise their rights under the Data Protection Laws and Regulations with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable). Taking into account the nature of the request, Pancake shall assist Customer by appropriate technical and organizational measures, to the extent legally required, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. Failing such action by Customer to comply with the requests of the Data Subject, Pancake will fulfill the request, insofar as possible, within a reasonable time.

4. PANCAKE PERSONNEL AND CONFIDENTIALITY

4.1. Confidentiality. Pancake shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and Service Data and have received appropriate training on their responsibilities.

4.2. Reliability. Pancake shall take commercially reasonable steps to ensure the reliability of any Pancake personnel who may have access to the Customer Personal Data or Service Data or Pancake personnel who may be engaged in the Processing of Personal Data.

4.3. Limitation of Access. Pancake shall ensure that Pancake's access to Personal Data and Service is limited to those Pancake personnel who need to know/access the relevant Personal Data and Service Data while performing Services in accordance with the Agreement.

4.4. Data Protection Officer. Pancake has appointed a data protection officer, who can be reached at contact@shortstacklab.com.

5. SUBPROCESSORS

5.1. Appointment of Subprocessors. Customer acknowledges and agrees that Pancake may engage third-party Subprocessors in connection with the provision of the Services. Pancake has entered into a written agreement

with each Subprocessor imposing on the Subprocessor the same obligations that apply to Processor with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Subprocessor under this Agreement.

5.2. List of Current Subprocessors. Pancake shall make available to Customer the current list of Subprocessors for the Services identified in Schedule 1 Appendix Annex III (List of Current Subprocessors).

5.3. Notification of New Subprocessors. Customer may find on Pancake's Privacy Policy page (https://www.shortstack.com/privacy-policy/), a mechanism to subscribe to notifications of new Subprocessors for each applicable Service, to which Customer may subscribe. If Customer subscribes, Pancake shall provide notification of a new Subprocessor(s) before authorizing any new Subprocessor(s) to Process Personal Data in connection with the provision of the applicable Services. Notification will be supplied in the form of an email to the email address submitted when subscribing for notification alerts at https://www.shortstack.com/privacy-policy/.

5.4. Objection Right for New Subprocessors. Customer may object to Pancake's use of a new Subprocessor by notifying Pancake promptly in writing (via an email to contact@shortstacklab.com) within fifteen (15) business days after receipt of Pancake's notice sent in accordance with the mechanism set out in Section 5.3.

5.5. In the event Customer objects to a new Subprocessor, as permitted in the preceding sentence, the objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the Subprocessor). If Pancake and Customer are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party. Customer shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

5.6. Liability. Where the Subprocessor fails to fulfill its data protection obligations, Pancake will remain liable to the Customer for the performance of such Subprocessor's obligations.

5.7. Disclosure of subprocessor agreements. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the SCCs to the data exporter, if requested by the data exporter according to the instructions under Section 5.3 (Notification of New Subprocessors). The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

6. OWNERSHIP OF SERVICE DATA

As between Customer and Pancake, Customer retains all right, title and interest in and to the Personal Data collected through use of the Service.

7. 7. SECURITY

7.1. Controls for the Protection of Customer Data. Pancake will implement and maintain the technical, physical, administrative and organizational measures to protect personal data against theft, unauthorized or unlawful acquisition, access, or processing, accidental loss, destruction, alteration, or damage as described in Schedule 1 - Appendix Annex II (Technical and Organisational Measures Including Technical and Organisational Measures To Ensure The Security Of The Data) of the DPA, as well as any other minimum security requirements required by laws generally applicable to Processors. Pancake will not materially decrease the overall security of the Services during a subscription term.

7.2. Third-Party Audits. The Parties acknowledge that Pancake uses external auditors to verify the adequacy of its security measures, including the security of the physical data centres from which Pancake provides its data processing services. This audit:

• will be performed at least annually;

• will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001;

• will be performed by independent third-party security professionals at Pancake's selection and expense; and

• will result in the generation of an audit report affirming that Pancake's data security controls achieve prevailing industry standards (including, without limitation, Service Organization Controls No. 2 (SOC2) in accordance with auditing standards in the Statements on Standards for Attestation Engagements No. 16 (SSAE16)) or such other alternative standards that are substantially equivalent to ISO 28001 ("Report").

Upon Customer's written request at reasonable intervals, Pancake shall make available to Customer that is not a competitor of Pancake (or Customer's independent, third-party auditor that is not a competitor of Pancake) a copy or a summary of Pancake's most recent Report, as applicable.

7.3. Customer responsibilities. Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials.

8. BREACH OF PERSONAL DATA SECURITY

8.1. After becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Pancake or its Subprocessors of which Pancake becomes aware (a "Customer Data Incident"), Pancake shall notify Customer without undue delay, within forty-eight (48) hours. Pancake shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Pancake deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Pancake's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or

Customer's Users.

8.2. Pancake's notice shall include the following information to the extent it is reasonably available to Pancake at the time of the notice, and Pancake shall update its notice as additional information becomes reasonably available:

• the dates and times of the Customer Data Incident;

• the facts that underlie the discovery of the Customer Data Incident;

• a description of the Personal Data involved in the Customer Data Incident; and

• the measures planned or underway to remedy or mitigate the vulnerability giving rise to the Customer Data Incident.

9. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Upon Customer's request, Pancake shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer Group Member by article 35 or 36 of the EU GDPR or equivalent provisions of any other Data Protection Laws and Regulations, in each case solely in relation 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 Pancake.

10. RETURN OR DESTRUCTION OF SERVICE AND COMPANY PERSONAL DATA

10.1. On termination of the Service Agreement upon the deletion of an account ("Termination of Service"), or on Customer's written request at any time, Pancake shall destroy any Service Data that is within its control.

10.2. Prior to the Termination of Service, Customer may export Service Data as a CSV file via their account.

10.3. Upon deletion of a list containing Personal Data collected by Customer through the Service, Service Data is destroyed within thirty (30) days.

10.4. Subject to Section 10.5, Customer may in its absolute discretion by written notice (via email) to Pancake at contact@shortstacklab.com within seven (7) days of the Termination of Service require Pancake to (a) return a complete copy of all Customer Personal Data to Customer; and (b) delete and procure the deletion of all other copies of Customer Personal Data Processed by Processor and any Subprocessor.

10.5. Processor and Subprocessors employed by Pancake may retain Customer Personal Data to the extent required by applicable laws and only to the extent and for such period as required by Applicable Laws and always provided that Pancake shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11. INTERNATIONAL DATA TRANSFERS

11.1. Data center locations. Customer acknowledges that Pancake may transfer and process Customer Data to and in the United States and anywhere else in the world where Pancake or its Sub-processors maintain data processing operations. Pancake shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and Regulations and this DPA.

11.2. Transfers outside of Europe. In connection with the Service, the parties anticipate that Pancake will transfer outside of the European Economic Area ("EEA"), Switzerland and United Kingdom to Pancake's Services environment located in the United States and Process Personal Data in respect of which the Customer or any member of the Customer Group may be a data controller, under applicable Data Protection Laws and Regulations.

11.3. Transfer mechanisms for data transfers. With respect to this transfer, Customer is the "exporter" and Pancake is the "importer" of the personal data. Pancake makes available the transfer mechanisms as follows, in order of precedence as set out in Section 11.3, to any transfers of

Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

11.3.1. EU SCCs set forth in Schedule 1 to this DPA shall apply to transfers subject to the EU GDPR.

11.3.2. EU SCCs set forth in Schedule 1 to this DPA shall apply to transfers subject to the Swiss DPA and be governed by the laws of and disputes shall be resolved before the courts of Switzerland.

11.3.3. UK SCCs found here shall apply to transfers subject to the UK GDPR and be populated with the relevant information set out in the Annexes to this DPA; and the UK SCCs shall be governed by the laws of and disputes shall be resolved before the courts of England and Wales.

11.3.4. EU-US Privacy Shield Framework. Pancake has certified its adherence to the EU-US Privacy Shield Framework as administered by the U.S. Department of Commerce, and will maintain the certification for the term of the Services Agreement. Pancake will provide at least the level of privacy protection required by the Privacy Shield principles.

11.3.5. Order of precedence. In the event that Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (a) the Standard Contractual Clauses and (b) Pancake's EU-U.S. Privacy Shield Framework self-certifications.

12. MISCELLANEOUS

12.1. Limitation of liability. Any claims brought in connection to this DPA (including, where applicable, the SCCs) shall be subject to the Terms and Conditions, including but not to limited to, the exclusions and limitations

set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under this DPA.

12.2. EU GDPR. With effect from 25 May 2018, Pancake will Process Personal Data in accordance with the EU GDPR requirements directly applicable to Pancake's provision of its Services.

12.3. Legal effect. This DPA shall only become legally binding between Customer and Pancake when the steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

12.4. Modification of DPA. This DPA may not be amended or modified except through a written Agreement signed by both Parties hereto.

12.5. Duration. The DPA will remain in force as long as Pancake Processes Personal Data on behalf of Customer under the Agreement.

LIST OF SCHEDULES

Schedule 1: Standard Contractual Clauses

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER

Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

PANCAKE LABORATORIES, INC

Signature: 

Print Name: Doug Churchill

Title: CEO

Date: January 14, 2021

SCHEDULE 1: Standard Contractual Clauses (Controllers to Processors)

For the purposes of the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organization: _____

Address: _____

Tel.: _____

Fax: _____

Email: _____

Other information needed to identify the organization:

_____

_____

(the data exporter)

And

Data importing organization:

Pancake Laboratories, Inc.

Address: 50 Washington Street, Suite 301, Reno, Nevada 89503, USA

Email: contact@shortstacklab.com

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the Standard Contractual Clauses (the Clauses) found in Schedule 1 in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in the Appendix.

Background
The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

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)[1] 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.

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

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

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 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[2] (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

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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) GENERAL WRITTEN AUTHORISATION 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 fifteen (15) business 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.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

(b) 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.

(c) 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 sub-processor) 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) Where the data exporter is established in an EU Member State: 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.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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[4];

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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.

(b) 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.

(c) 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.).

(d) 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.

(e) 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 the EU Member State in which the data exporter 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 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.

(f) The Parties agree that those shall be the courts of the Republic of Ireland.

(g) 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.

(h) The Parties agree to submit themselves to the jurisdiction of such courts.

(i)

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter:

Name:_____

_____

Address:_____

_____

_____

Contact person's name, position and contact details:_____

_____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

_____

Signature and date:

Role (controller/processor): Controller

Data importer:

Name: Pancake Laboratories, Inc

Address: 50 Washington Street, Suite 301, Reno, Nevada 89503, USA

Contact person's name, position and contact details:

Adam Hemler

President of Sales

adam@shortstacklab.com

Activities relevant to the data transferred under these Clauses: Data importer operates a cloud-based marketing services platform, including online forms, contests and interactive marketing features. The data importer will host and process Personal Data in the course of providing its cloud-based Services to data exporter pursuant to the Agreement.

Signature: 

Print Name: Doug Churchill
Title: CEO
Date: January 14, 2021

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Pancake Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

Data exporter's contacts and other end users including Data exporter's collaborators, customers, prospects, and suppliers (who are natural persons).

Employees, agents, advisors, freelancers of data exporter (who are natural persons).

Categories of personal data transferred

The personal data transferred concern the following categories of data: Personal Data, to the extent of which is determined and controlled by the Data exporter in its sole discretion, may be submitted, stored, sent, or received by end users via the Pancake Service submitted to the Pancake Services, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Professional information (Title, Position, Employer)
- Contact information (email, phone, physical address)
- Personal life data
- Application integration data
- System Usage data
- Other electronic data

Special categories of data

The personal data transferred concern the following special categories of data: Data exporter may submit special categories of data to the Pancake Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information possibly revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

The personal data transferred will be subject to the following basic processing activities:

The data importer will host and process Personal Data in the course of providing its cloud-based Services to data exporter pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

To provide Services to data exporter pursuant to the Agreement, including technical, customer support, operations and administrative services.

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

Until Termination of Service, which results in a deletion of data exporter's account, or on data exporter's written request that Pancake destroy any Personal Data that is within its control.

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

Until Termination of Service, which results in a deletion of data exporter's account, or on data exporter's written request that Pancake destroy any Personal Data that is within its control.

C. COMPETENT SUPERVISORY AUTHORITY

Republic of Ireland's Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland
Website: https://www.dataprotection.ie/
Contact form: https://www.dataprotection.ie/en/contact/how-contact-us

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

Pancake observes the technical and organizational security measures found at https://www.shortstack.com/security-faqs/. Pancake reserves the right to modify or update these practices at its sole discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors as listed at https://www.shortstack.com/shortstack-subprocessors/ and updated from time to time after notice from Pancake.