USERFLOW DATA PROCESSING ADDENDUM
(Revision May 2024)

This Data Processing Addendum ("**DPA**") forms part of the Terms of Service and Privacy Policy or other written or electronic agreement between Userflow and Customer for the purchase and/or use of online services (including associated Userflow mobile components) from Userflow (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of Customer's Authorized Affiliates, if and to the extent Userflow processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Userflow may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, and 3 (including Annex I-III and the UK and Swiss addendum).

2. To complete this DPA, Customer must:

    a. Complete the information in the signature box and sign on Page 11.

    b. Complete the information in the signature box and sign on Page 29.

    c. Complete the information in the signature box and sign on Page 35.

3. Send the completed and signed DPA to Userflow at support@userflow.com.

Upon receipt of the validly completed DPA by Userflow at this email address, Userflow will complete and sign the DPA and the Standard Contractual Clauses in Schedule 3 as the data

importer. The DPA will be returned to Customer, whereafter this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Userflow entity that is party to the Agreement is party to this DPA.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means (a) any entity on whose behalf Customer obtained the Userflow Services, and/or (b) 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.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Userflow, but has not signed its own Agreement with Userflow and is not a "Customer" as defined under the Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means what is described in the Userflow Privacy Policy as "your data", "your info" or similar terms.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states ("GDPR"), Switzerland ("Swiss DPA") and the United Kingdom ("UK GDPR"), applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

“Processing” (including its various forms) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, 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.

“Processor” means the entity which Processes Personal Data on behalf of the Controller.

“Security and Privacy Documentation” means Userflow’s security overview, as updated from time to time, and accessible via https://userflow.com/policies/security, and Userflow’s Privacy Policy, as updated from time to time, and accessible via https://userflow.com/policies/privacy, or as otherwise made reasonably available by Userflow

"**Standard Contractual Clauses (SCC)**" means the standard contractual clauses for Customer Data that is transferred to a country outside the EEA not recognized as providing an adequate level of protection for personal data as described in the GDPR, which are attached as Schedule 3. By signing this DPA and using Userflow’s services to transfer data, Customer agrees to the Standard Contractual Clauses, if applicable.

“Sub-processor” means any Processor engaged by Userflow.

“Supervisory Authority” means an independent public authority which is established by an EEA State pursuant to the GDPR, the UK’s Information Commissioner’s Office and/or the Swiss Federal Data Protection and Information Commissioner.

“Userflow” means the Userflow entity which is a party to this DPA, as specified in the section “HOW THIS DPA APPLIES” above, being Userflow, Inc., a Delaware Corporation.

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, Customer is the Controller, Userflow is the Processor and that Userflow will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” 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 Userflow’s Processing of Personal Data. Userflow shall treat Personal Data as confidential information and shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customers and/or Authorized Affiliates in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by Userflow 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 2 (Details of the Processing) to this DPA.

3. DATA SUBJECT REQUESTS

Userflow shall, to the extent legally permitted, promptly notify Customer if Userflow receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (“Data Subject Request”). Taking into account the nature of the Processing, Userflow shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services,

does not have the ability to address a Data Subject Request, Userflow shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Userflow is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Userflow's provision of such assistance.

4. USERFLOW PERSONNEL

4.1 Confidentiality. Userflow shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Userflow shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. Userflow shall take commercially reasonable steps to ensure the reliability of any Userflow personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Userflow shall ensure that Userflow's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 Data Protection Officer. Based on Userflow's processing activities, Userflow is not required to appoint a Data Protection Officer. Userflow reserves the right to voluntarily appoint a Data Protection Officer in the future. For questions about this DPA, GDPR compliance, data privacy, Data Privacy Framework, or any other privacy issues please send an email to support@userflow.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Userflow's Affiliates may be retained as Sub-processors; and (b) Userflow and Userflow's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Userflow or a Userflow Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. Userflow shall make available to Customer the current list of Sub-processors for the Userflow Services. Such

Sub-processor lists shall include the identities of those Sub-processors and their country of location ("**Sub-processor Documentation**"). Customer may find on Userflow's webpage at https://userflow.com/policies/subprocessors the Sub-processor Documentation. Userflow, through notification to the Customer shall provide notification of a new Sub-processor(s) before authorizing any new Sub- processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3 Objection Right for New Sub-processors. Customer may object to Userflow's use of a new Sub-processor by notifying Userflow promptly in writing within ten (10) business days after receipt of Userflow's notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Userflow will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected- to new Sub-processor without unreasonably burdening the Customer. If Userflow is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Agreement with respect only to those Services which cannot be provided by Userflow without the use of the objected-to new Sub-processor by providing written notice to Userflow. Userflow will refund Customer any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4 Liability. Userflow shall be liable for the acts and omissions of its Sub-processors to the same extent Userflow would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1 Controls for the Protection of Customer Data. Userflow shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security and Privacy Documentation. Userflow regularly monitors compliance with these measures. Userflow will not materially decrease the overall security of the Services during a subscription term.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Userflow maintains security incident management policies and procedures specified in the Security and Privacy Documentation and the Agreement. Userflow shall, notify Customer without undue delay, and in compliance with applicable laws, 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 Userflow or its Sub-processors of which Userflow becomes aware (a "**Customer Data Incident**"). Userflow shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Userflow deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Userflow's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Authorized Affiliates.

8. RETURN AND DELETION OF CUSTOMER DATA

Userflow shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security and Privacy Documentation.

9. AUTHORIZED AFFILIATES

9.1 Contractual Relationship. The parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Userflow and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, by Customer entering into this DPA, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

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

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Userflow, it shall to the extent required under applicable Data Protection Laws and

Regulations be entitled to exercise the rights and see remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or see any remedy under this DPA against Userflow directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or see any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Userflow and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Userflow, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability set forth in the Agreement, and such limitations apply to the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

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

Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

11. EUROPEAN SPECIFIC PROVISIONS

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

11.2 Data Protection Impact Assessment. With effect from May 25, 2018, upon Customer's request, Userflow shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Userflow. Userflow shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR.

11.3 Transfer mechanisms for data transfers. Subject to the additional terms in Schedule 1, Userflow makes available the transfer mechanisms listed below which shall apply 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:

1. The Standard Contractual Clauses set forth in Schedule 3 to this DPA apply to all Userflow services (the "**SCC Services**"), subject to the additional terms in Section 1 of Schedule 1.
2. 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.
3. Article 49(1)(b) of the GDPR (the transfer is necessary for the performance of a contract), and the equivalent provisions in the Data Protection Laws and Regulations, applies to transfers of personal data made in connection with product fulfilment, in connection with surveys, newsletters and blogs, in connection with providing Customer support to prospective Customers, and in connection with recruiting for prospective new hires.

12. PARTIES TO THIS DPA

The Section "HOW THIS DPA APPLIES" specifies which Userflow entity is party to this DPA. In addition, Userflow, Inc. is a party to the Standard Contractual Clauses in Schedule 3. Notwithstanding the signatures below of any other Userflow entity, such other Userflow entities are not a party to this DPA or the Standard Contractual Clauses.

13. LEGAL EFFECT

This DPA shall only become legally binding between Customer and Userflow when the formalities steps set out in the Section “HOW TO EXECUTE THIS DPA” above have been fully completed.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers
Schedule 2: Details of the Processing
Schedule 3: Standard Contractual Clauses

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER
Signature:_____
Customer Legal Name:
Print Name:
Title:
Date: _____

USERFLOW, INC.
Signature:_____
Print Name:
Title:
Date: _____

SCHEDULE 1
TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

ADDITIONAL TERMS FOR SCC SERVICES

1. Customers covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Section 1 of this Schedule 1 apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and (ii) all Affiliates, including, but not limited to, Authorized Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Agreements for the SCC Services. For the purpose of the Standard Contractual Clauses and this Section 1, the aforementioned entities shall be deemed "data exporters".

Instructions. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Userflow for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of the applicable Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement; (b) Processing initiated by Users in their use of the SCC Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

Appointment of new Sub-processors and List of current Sub-processors. Pursuant to the applicable the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) Userflow's Affiliates may be retained as Sub-processors; and (b) Userflow and Userflow's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services. Userflow shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA.

1.4 Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to the applicable Standard Contractual Clauses, Customer acknowledges and expressly agrees that Userflow may engage new Sub-processors as described in Sections 5.2 and 5.3 of the DPA.

1.5. Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by Userflow to Customer pursuant to the applicable Standard Contractual Clauses may have all commercial information, or clauses unrelated to the

Standard Contractual Clauses or their equivalent, removed by Userflow beforehand; and, that such copies will be provided by Userflow, in a manner to be determined in its discretion, only upon request by Customer.

1.6. Audits and Certifications. The parties agree that the audits described in the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Userflow shall make available to Customer that is not a competitor of Userflow (or Customer's independent, third-party auditor that is not a competitor of Userflow) information regarding Userflow's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Security and Privacy Documentation to the extent Userflow makes them generally available to its customers. Customer may contact Userflow in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Userflow for any time expended for any such on-site audit at Userflow's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Userflow shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Userflow. Customer shall promptly notify Userflow with information regarding any non-compliance discovered during the course of an audit.

1.7. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in the applicable Standard Contractual Clauses shall be provided by Userflow to Customer only upon Customer's request.

1.8. Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

SCHEDULE 2
DETAILS OF THE PROCESSING

Nature and Purpose of Processing
Userflow will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the DPA, and as further instructed by Customer in its use of the Services.

Duration of Processing
Subject to Section 8 of the DPA, Userflow will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects
Customer may submit Personal Data to the Services, the categories, extent and detail of which is determined and controlled by Customer in its sole discretion.

Type of Personal Data
Customer may submit Personal Data to the Services, the type, extent and detail of which is determined and controlled by Customer in its sole discretion.

SCHEDULE 3
STANDARD CONTRACTUAL CLAUSES
(Module 2: controller to processor)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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 - Optional

Docking clause - Not used

SECTION II – OBLIGATIONS OF THE PARTIES

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent

possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and

monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[1] (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:

[1] 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.

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s). 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 10 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.[2] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

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

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

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

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

(c) 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.

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

(e) 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[3];

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

[3] 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.

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

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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] 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) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) 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.

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

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature: _____

(Stamp of the organization)

On behalf of the data importer:
Name (written out in full):
Position:
Address: 548 Market St PMB 69598, San Francisco, CA 94104-5401

Signature: _____

(Stamp of the organization)

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter(s)

[*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: The entity identified as Customer in the Addendum or such other agreement between Userflow and Customer

Address: The Address for the Customer as specified in the DPA or other such agreement

Contact person's name, position and contact details: The contact details associated with the DPA or other such agreement

Activities relevant to the data transferred under these Clauses: The activities specified in the Addendum

Signature and date: By using signing the DPA and using Userflow's services to transfer data to Third Countries, the exporter will be deemed to have signed Annex 1

Role (controller/processor): Controller

Data importer(s):

[*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Userflow, Inc.

Address: 548 Market St PMB 69598, San Francisco, CA 94104-5401, USA

Contact person's name, position and contact details: Sudhakar Mylsamy, CTO, support@userflow.com

Activities relevant to the data transferred under these Clauses: Userflow is a cloud-based software-as-a-service provider of user onboarding software, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Signature and date: By signing the DPA and processing the data exporter's data on data exporter's instructions, the data importer will be deemed to have signed this Annex I

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter and/or Data Subjects (as directed by data exporter), may submit Personal Data to the Services, the categories, extent and detail of which is determined and controlled by the data exporter in its sole discretion. This could be, but is not limited to the following categories of Data Subjects:

- Prospects, customers business partners and vendors (who are natural persons) of data exporter;
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors;
- Employees, agents, advisors, independent contractors, members and/or freelancers of data exporter; and/or
- Other categories of Data Subjects as expressly determined by the data exporter.

Categories of personal data transferred

Data exporter and/or Data Subjects (as directed by data exporter) may submit Personal Data to the Services, the type, extent and detail of which is determined and controlled by the data exporter and/or the Data Subject in its sole discretion.

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

Data exporter and/or Data Subjects (as directed by data exporter) may submit Sensitive data to the Services, the type, extent and detail of which is determined and controlled by the data exporter and/or the Data Subject in its sole discretion. Userflow takes the security and privacy of data very seriously. The restrictions and safeguards that apply to all data, including any sensitive data, can be found in Userflows's Privacy Policy and Security Policy,

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

Data exporter and/or Data Subjects (as directed by data exporter) may submit Personal Data to the Services either once, or on a continuous basis (for example by making changes to Personal Data) as determined and controlled by the data exporter and/or the Data Subject in its sole discretion.

Nature of the processing

Userflow processes Personal Data only as necessary to perform the Services and only performs

the type(s) of processing as instructed by the data exporter and/or Data Subject and only pursuant to the Agreement, the DPA and these Clauses.

Purpose(s) of the data transfer and further processing

The purposes of the processing are determined solely by the data exporter and/or Data Subject in its sole discretion.

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

Subject to any other terms allowing or requiring longer retention, and subject to Userflow's

normal data retention policies, Userflow only processes personal data for the duration of the Agreement, unless the data is deleted prior thereto by the data exporter and/or Data Subject.

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

Userflow transfers Personal Data to sub-processors as set forth in the Subprocessors section of Userflow's Privacy Regulations Reference. See https://userflow.com/policies/privacy-regulations and https://userflow.com/policies/subprocessors.

C. COMPETENT SUPERVISORY AUTHORITY

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

For the purposes of the Standard Contractual Clauses, 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. 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 - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the SCC Services, as described in the Security and Privacy Documentation applicable to the specific SCC Services purchased by data exporter. Data Importer will not materially decrease the overall security of the SCC Services during a subscription term.

An overview of Userflows security mechanisms can be found here https://userflow.com/policies/security.

ANNEX III – LIST OF SUB-PROCESSORS

Data importer establishes data processing agreements with all of its subprocessors that handle personal data. You can find out more about each subprocessor here https://userflow.com/policies/subprocessors.

UK AND SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

(a) This Addendum amends the Standard Contractual Clauses to the extent necessary so they operate for transfers made by the data exporter to the data importer, to the extent that the UK GDPR or Swiss DPA (as defined in the Userflows Data Processing Addendum) apply to the data exporter’s processing when making that transfer.

(b) The Standard Contractual Clauses shall be amended with the following modifications:

i. references to "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR or Swiss DPA (as applicable);

ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the UK GDPR or Swiss DPA (as applicable);

iii. references to Regulation (EU) 2018/1725 shall be removed;

iv. references to "EU", "Union" and "Member State" shall be replaced with references to the "UK" or "Switzerland" (as applicable); v. Clause 13(a) and Part C of Annex II are not used and the "competent supervisory authority" shall be the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable); vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);

vii. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and

viii. to the extent the UK GDPR applies to the processing, Clause 18 shall be replaced to state: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts”; and

ix. to the extent the Swiss DPA applies to the processing, Clause 18 shall be replaced to state: “Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts”

DATA EXPORTER
Name:
Signature_____

DATA IMPORTER
Name:
Signature_____