

## Data Processing Addendum for the Workato Platform

Last Updated: May, 2022

This Data Processing Addendum (“**DPA**”) forms part of Workato’s Terms of Service (the “**Agreement**”) entered into by and between the Account Holder (**Account Holder**) and Workato, Inc. (“**Workato**”). Any terms not defined in this DPA shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall take precedence with regard to the subject matter of this DPA.

### 1. Definitions

(a) “**Anonymous Data**” means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable Data Subject.

(b) “**Authorized Individual**” means an employee of Workato who has a need to know or otherwise access Personal Data to enable Workato to perform its obligations under this DPA or the Agreement or an Authorized Sub-Processor.

(c) “**Authorized Sub-Processor**” means another Processor engaged by Workato, and who is either (1) listed as a sub-Processor on Workato’s List (as defined in Section 4.2 below) and/or (2) authorized by Account Holder to do so under Section 4 of this DPA.

(d) “**CCPA**” means the California Consumer Privacy Act and implementing regulations, as may be amended from time to time.

(e) “**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data, including as applicable any “business” as defined under the CCPA.

(f) “**Data Protection Laws**” means (i) the CCPA; (ii) the GDPR (as defined below) and related data protection and privacy laws of the member states of the European Economic Area; (iii) the Data Protection Act 2018 of the United Kingdom (“UK GDPR”); and (iv) the Swiss Federal Act on Data Protection (1992); and (v) the Singapore Personal Data Protection (Amendment) Act 2020; each as applicable and as amended, repealed, consolidated or replaced from time to time.

(g) “**Data Subject**” means an identified or identifiable person to whom Personal Data relates.

(h) “**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.

(i) “**Instruction**” means a direction, either in writing, in textual form (e.g., by e-mail) or by using a software or online tool, issued by Account Holder to Workato and directing Workato to Process Personal Data.

(j) “**Personal Data**” means any information relating to Data Subjects. Personal Data does not include Anonymous Data.

(k) “**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.

(l) “**Process**” or “**Processing**” means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

(m) “**Processor**” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Account Holder, including as applicable any “service provider” as defined under the CCPA.

(n) “**Services**” means the services provided by Workato pursuant to the Agreement.

(o) **“Standard Contractual Clauses”** means (i) where the GDPR applies, the standard contractual clauses for the transfer of Personal Data to third countries approved by the European Commission’s decision 2021/914/EC of June 4, 2021, as currently set out at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) (the “EU SCCs”); (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 (the “UK SCCs”).

(p) **Supervisory Authority** means an independent public authority which is established by a member state of the European Economic Area and the United Kingdom.

## 2. Relationship of the Parties; Processing of Data

(a) Account Holder acknowledges and agrees that with regard to the processing of Account Holder Usage Data and product support data, Account Holder may act either as a controller or processor and Workato is an independent Controller, not a joint controller with Account Holder. Workato has the right to Process Usage Data or support ticket data relating to or obtained in connection with the operation, support, or use of the Services for its legitimate internal business purposes, including, but not limited to: (a) billing, tax, and audit support, (b) to provide, optimize, maintain, develop and improve the Services, (c) to investigate fraud, wrongful or unlawful use of the Services, and (d) as required by applicable law or regulation. In such instances, this DPA shall not apply. Workato will Process such Personal Data in compliance with applicable Data Protection Laws and Section 6(b)(1) of this DPA.

(b) The rights and obligations of the Account Holder with respect to the Processing of Personal Data are described herein. Account Holder shall, in its use of the Services, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with the Data Protection Laws. Account Holder shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Account Holder’s instructions will not cause Workato to be in breach of the Data Protection Laws. Account Holder is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Workato by or on behalf of Account Holder, (ii) the means by which Account Holder acquired any such Personal Data, and (iii) the instructions it provides to Workato regarding the Processing of such Personal Data. Account Holder shall not provide or make available to Workato any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services and shall indemnify Workato from all claims and losses in connection therewith.

(c) Workato shall Process Personal Data only (i) for the purposes set forth in the Agreement, this DPA, including Schedule 1 (ii) in accordance with the terms and conditions set forth in this DPA and any other documented Instructions provided by Account Holder, and (iii) in compliance with the Data Protection Laws. Account Holder hereby instructs Workato to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Account Holder in its use of the Services. If Workato is unable to Process Personal Data pursuant to the Instructions due to legal requirements under applicable laws, Workato shall inform the Account Holder of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Workato shall also immediately inform the Account Holder if, in its opinion, an Instruction infringes the applicable laws, including the Data Protection Laws. In such case, Workato will cease all Processing of the affected Personal Data (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Account Holder issues new Instructions with which Workato is able to comply. If this provision is invoked, Workato will not be liable to Account Holder under the Agreement for failure to perform the Services until such time as Account Holder issues new Instructions.

(d) The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data Processed and categories of Data Subjects, are described in Schedule 1 to this DPA.

(e) Following completion of the Services, at Account Holder’s choice, Workato shall return or delete the Personal Data, except as required to be retained by the Data Protection Laws or other applicable laws, or for the limited scope and purposes specified in section 11. If Account Holder and Workato have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 and 16 of the Standard Contractual Clauses shall be provided by Workato to Account Holder only upon Account Holder’s request.

(f) To the extent Workato's Processing of Personal Data is subject to the CCPA, (i) Workato shall not (1) retain, use, or disclose Personal Data other than as provided for in the Agreement, as needed to perform the Services, to build or improve the quality of the Services to detect security incidents, to protect against fraudulent or illegal activity, to retain sub-Processors in compliance with Section 4, or as otherwise permitted by the CCPA; or (2) sell Personal Data.

### 3. Authorized Individuals

(a) Workato shall take commercially reasonable steps to limit access to Personal Data to only Authorized Individuals.

(b) Workato shall ensure that all Authorized Individuals are made aware of the confidential nature of Personal Data and have executed confidentiality agreements

### 4. Authorized Sub-Processors

(a) Account Holder acknowledges and agrees that Workato may (i) engage its Affiliates and other Authorized Sub-Processors to access and Process Personal Data in connection with the Services and (ii) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data.

(b) Workato's current Authorized Sub-Processors include (i) the third-party Sub-Processors; and (ii) its Affiliates listed at [www.workato.com/legal/sub-processors](http://www.workato.com/legal/sub-processors) (such URL may be updated by Workato from time to time), (the "List"), as updated from time to time. At least thirty (30) days before enabling any third-party Sub-Processors other than Authorized Sub-Processors to access or participate in the Processing of Personal Data, Workato will add such third-party Sub-Processors and Affiliates to the List and notify Account Holder of such updates via email. Account Holder may object to such an engagement in writing within ten (10) days of receipt of the aforementioned notice by Account Holder.

(i) If Account Holder reasonably objects to an engagement in accordance with Section 4(b), Workato may provide Account Holder with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If Workato, in its sole discretion, does not provide any such alternative(s), or if Account Holder does not agree to any such alternative(s) if provided, either party may terminate this DPA and the Agreement upon written notice. Termination shall not relieve Account Holder of any fees owed to Workato under the Agreement.

(ii) If Account Holder does not object to the engagement of a third-party Sub-Processor in accordance with Section 4(b) within ten (10) days of notice by Workato, that third-party Sub-Processor will be deemed an Authorized Sub-Processor for the purposes of this DPA.

(c) Workato shall, by way of contract or other legal act under European Union, European Union member state or United Kingdom law (including Standard Contractual Clauses), ensure that every Authorized Sub-Processor is subject to obligations regarding the Processing of Personal Data that are no less protective than those to which the Workato is subject under this DPA.

(d) Workato shall be liable to Account Holder for the acts and omissions of Authorized Sub-Processors to the same extent that Workato would itself be liable under this DPA had it conducted such acts or omissions. If Account Holder and Workato have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations in Section 4.2 will constitute Account Holder's prior written consent to the subcontracting by Workato of the Processing of Personal Data if such consent is required under the Standard Contractual Clauses; and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Workato to Account Holder pursuant to Clause 9(c) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Workato beforehand, and that such copies will be provided by the Workato only upon request by Account Holder.

### 5. Security and Confidentiality of Personal Data

(a) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Workato shall maintain appropriate technical and organizational measures to ensure a

level of security appropriate to the risk of Processing Personal Data. Workato shall, taking into account the nature of the Processing and the information available to Workato, provide Account Holder with reasonable cooperation and assistance where necessary for Account Holder to comply with Account Holder's obligations pursuant to Article 32 GDPR or equivalent provision of the Data Protection Laws. More specific security and privacy measures implemented by Workato include, but are not limited to, those set forth in Schedule 2.

## **6. Transfers of Personal Data**

(a) Any transfer of Personal Data made subject to this DPA from member states of the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of these countries shall, to the extent such transfer is subject to such laws and regulations, be undertaken by Workato through the Standard Contractual Clauses set forth in Schedule 3 or Schedule 4 or Schedule 5 to this DPA, as applicable.

(b) For data transfers subject to the EU SCCs, the EU SCCs will be deemed entered into and completed as follows:

(i) Module One (Controller to Controller) of the EU SCCs will apply where Workato Processes Account Holder Usage Data or support ticket data.

(ii) Module Two (Controller to Processor) of the EU SCCs will apply where Workato is a Processor and Account Holder is a Controller.

## **7. Rights of Data Subjects**

(a) Workato shall, to the extent permitted by law, promptly notify Account Holder upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, restriction of Processing, erasure, data portability, restriction of or objection to Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Workato receives a Data Subject Request in relation to Personal Data, Workato will advise the Data Subject to submit their request to Account Holder and Account Holder will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.

(b) Workato shall, at the request of the Account Holder, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Account Holder in complying with Account Holder's obligation to respond to such Data Subject Request, where possible, provided that (i) Account Holder is itself unable to respond without Workato's assistance and (ii) Workato is able to do so in accordance with all applicable laws, rules, and regulations.

## **8. Actions and Access Requests**

(a) Workato shall, taking into account the nature of the Processing and the information available to Workato, provide Account Holder with reasonable cooperation and assistance where necessary for Account Holder to comply with obligations applicable to it under the Data Protection Laws to conduct a data protection impact assessment, provided that Account Holder does not otherwise have access to the relevant information.

(b) Workato shall, taking into account the nature of the Processing and the information available to Workato, provide Account Holder with reasonable cooperation and assistance with respect to Account Holder's cooperation and/or prior consultation with any Supervisory Authority, where necessary and/or where required by the Data Protection Laws.

## **9. Audit Rights**

(a) Account Holder may audit Workato's compliance with the terms of the Agreement and this DPA once a year). If a third-party is to conduct the audit, the third-party must be mutually agreed to by Account Holder and Workato and such third-party must execute a confidentiality agreement with Workato before the audit is conducted.

(b) To request an audit, Account Holder must submit a detailed proposed audit plan to Workato at least thirty (30) days in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Workato will review the proposed audit plan and communicate any concerns or questions to Account Holder. Workato will cooperate with Account Holder to agree on a final audit plan.

(c) The audit must be conducted during regular business hours and subject to applicable Workato policies. The audit may not unreasonably interfere with Workato's business operations. If the information required for such an audit is not contained in a SOC 2 Type 2 or similar report, Workato will make reasonable efforts to provide the requested information to the auditor.

(d) Account Holder will provide Workato any audit reports generated in connection with any audit under this section, unless prohibited by law. Account Holder may use the audit reports only for the purposes of meeting its regulatory requirements and/or confirming compliance with the requirements of the Agreement and this DPA. The audit report(s) and any information obtained by Account Holder under this section are Workato's Confidential Information under the terms of the Agreement.

(e) Any audits conducted shall be at Account Holder's expense. Any request for Workato to provide assistance with an audit is considered a separate service if such audit assistance requires the use of additional or different resources than those Workato would typically utilize when providing such audit assistance. Workato will seek Account Holder's prior written approval and agreement to pay any related fees before performing such audit assistance.

## **10. Incident Management and Breach Notification**

(a) In the event of a confirmed Personal Data Breach, Workato shall, within 48 hours, inform Account Holder of the Personal Data Breach and take such steps as Workato in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Workato's reasonable control).

(b) In the event of a confirmed Personal Data Breach, Workato shall, taking into account the nature of the Processing and the information available to Workato, provide Account Holder with reasonable cooperation and assistance necessary for Account Holder to comply with its obligations under the applicable Data Protection Laws with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

(c) As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Workato, Workato will also provide Account Holder with (i) a description of the nature and reasonably anticipated consequences of the Personal Data Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of Personal Data that were the subject of the Personal Data Breach. Account Holder agrees to coordinate with Workato on the content of Account Holder's intended public statements or required notices for the affected Data Subjects and/or notices to the relevant Supervisory Authority regarding the Personal Data Breach.

(d) The obligations described in Sections 10(a) and 10(b) shall not apply in the event that a Personal Data Breach results from the actions or omissions of Account Holder.

## **11. Limitation of Liability; Expenses**

(a) The total liability of each of Account Holder and Workato (and their respective employees, directors, officers, Affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement.

(b) Workato will be entitled to be reimbursed by Account Holder, to the extent legally permitted, for reasonable costs and expenses arising from any assistance by Workato in Sections 7, 8(a), 8(b) and 9.

## **12. Communications**

The person(s) authorized to issue instructions to Workato under this DPA are those specified as contacts in the order form. Outside of Instructions issued within the Workato Platform by authorized Personnel, any

additional Instructions must be received only from designated individuals specified in the applicable Order Form. In the event that these contacts change or otherwise become permanently unavailable, the respective party shall communicate such change immediately in writing.

### 13. Miscellaneous

If there is any conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail with respect to Personal Data that is subject to EU GDPR or UK GDPR.

#### WORKATO, INC.

#### COMPANY

By: \_\_\_\_\_

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

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

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

By: \_\_\_\_\_

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

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

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



## Schedule 1 – Details of Processing

### Section A: List of Parties

**Data Importer:** Workato, Inc.

**Data Exporter:** Account Holder

**Address:** 215 Castro Street, Suite 300, Mountain View, CA 94041

**Address:** [INSERT]

**Contact person's name, position and contact details:** Chief Information Security Officer, privacy@workato.com

**Contact person's name, position and contact details:** [INSERT]

**Role:** processor/controller

**Role:** controller

### Section B: Description of Processing/Transfer

**Categories of Data Subjects:** Account Holder may submit Personal Data to the Service, the extent to which is determined and controlled by the Account Holder in its sole discretion, and which may include, but not limited to Personal Data relating to the following categories of Data Subjects:

Account Holder employees, independent contractors, agents, advisors and freelancers.

Account Holder prospects, customers, business partners and vendors, or their respective employees and contract persons.

**Categories of Personal Data:** The Personal Data included in the Account Holder Data uploaded to the Services by Account Holder for Processing under Account Holder's Accounts, the extent to which is determined and controlled by the Account Holder in its sole discretion, which may include, but is not limited to the following categories of Personal Data:

- First and last name
- IP Address
- Email

**Sensitive data transferred (if applicable):** The contents of the Personal Data are varied and under the data exporter's control, but may, from time to time, include sensitive data under the relevant Data Protection Laws. Data importer provides facilities for special handling of sensitive data, including data retention periods and data masking. See Processor's technical and organizational measures outlined in Schedule 2.

**The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):** Frequency of the transfer is configurable in a self-service manner by the Data exporter and is a continuous basis for the duration of the Agreement.

**Nature and Purpose of Processing:** Workato provides a flexible business integration and automation service. Workato will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Account Holder in its use of the Services.

**Frequency and Duration of Processing:** Subject to Section 2(d) of the DPA, Workato will Process Personal Data for the duration of the Agreement. Personal Data submitted to the data importer is retained for a limited period of time, in accordance with its published data retention policies. In general, the retention period is 30 days unless otherwise configured by the data exporter, and in no case exceeds 90 days.

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:** As specified on importer's current Subprocessor Page.

## Schedule 2 – Data Security Measures

Maintains an information security program which is approved by its management and regularly reviewed and updated accordingly.

Restricts access to Personal Data to Authorized Individuals who provide authentication that uniquely identifies them.

Restricts Authorized Individuals' rights to access or modify Personal Data based on business role and need.

Reviews access and authorization rights for Authorized Individuals regularly. Access or authorization rights are withdrawn or modified, as appropriate, promptly upon termination or change of role for such Authorized Individuals.

Ensures that physical access to systems storing or Processing Personal Data is appropriately secured and monitored.

Encrypts Personal Data both at rest and in transit, using industry standard protocols and encryption algorithms.

Has implemented and maintains secure coding and development standards, incorporating security and privacy considerations.

Ensures that its personnel receive regular security and privacy training so that they are aware of their roles and responsibilities with regard to the treatment and protection of Personal Data.

Segregates internal systems storing or processing Personal Data from public networks.

Has implemented anti-malware on systems that do or may Process Personal Data.

Has implemented monitoring and alerting capabilities on its systems.

Evaluates its systems for vulnerabilities and deploys required security updates on a schedule based on risk and severity.

Regularly tests the security of its systems including an annual penetration test performed by a qualified third party.

Evaluates the security and privacy practices of all Authorized Sub-Processors. All Authorized Sub-Processors are required to implement and maintain the same or substantially similar technical and organizational measures and assume the same responsibilities and obligations as those required of Processor under this DPA.

Deploys redundant services and engages in practices including regular backups designed to provide continued availability and access to data despite disruptions to its infrastructure.

Maintains an incident response plan and commits to providing required notifications in case of a confirmed Personal Data Breach without undue delay.

Maintains systems and processes for complying with data privacy requirements including limited retention and processing of requests from Data Subjects.



## Schedule 3

### CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES

#### ANNEX

to the

#### COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

#### ANNEX

### 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)<sup>1</sup> 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    Clause 7 – Optional*

*Docking clause INTENTIONALLY DELETED*

## 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, organization, 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 authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

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

### **8.7. Sensitive data**

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

### **8.8. Onward transfers**

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

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

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

### **8.9. Documentation and compliance**

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

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

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

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

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

## *Clause 9*

### *Use of sub-processors*

(a) [OPTION 2: 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 thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.]

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

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

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

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

## *Clause 10*

### *Data subject rights*

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

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

nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

## *Clause 11*

### *Redress*

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

(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 I 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 I, 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;

(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 I, 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 I 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 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.

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

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

### *Clause 17*

#### *Governing law*

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

### *Clause 18*

#### *Choice of forum and jurisdiction*

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

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

- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

## ANNEX I

### A. LIST OF PARTIES

The contents of Section A of Schedule 1 are incorporated herein.

### B. DESCRIPTION OF TRANSFER

The contents of Section B Schedule 1 are incorporated herein.

### C. COMPETENT SUPERVISORY AUTHORITY

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

The Irish Data Protection Commission will be the competent supervisory authority.



## ANNEX II

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.*

See Schedule 2 for description of technical and organisational measures.

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.*

All Authorized Sub-Processors are required to implement and maintain the same or substantially similar technical and organizational measures, responsibilities and obligations as those required of the Processor under this DPA.

## **Schedule 4**

### **CONTROLLER TO CONTROLLER STANDARD CONTRACTUAL CLAUSES**

### **ANNEX**

to the

### **COMMISSION IMPLEMENTING DECISION**

**on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

### **ANNEX**

## **STANDARD CONTRACTUAL CLAUSES**

### **SECTION I**

#### *Clause 1*

#### *Purpose and scope*

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

(b) The Parties:

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

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

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

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

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

#### *Clause 2*

#### *Effect and invariability of the Clauses*

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

(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 8.5 (e) and Clause 8.9(b);
- (iii) N/A
- (iv) Clause 12(a) and (d);
- (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 – Optional*

#### *Docking clause INTENTIONALLY DELETED*

## 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. 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. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

#### **8.2. Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

- (i) of its identity and contact details;
- (ii) of the categories of personal data processed;
- (iii) of the right to obtain a copy of these Clauses;
- (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.3. Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

#### 8.4. Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

#### 8.5. 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they 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 subject. 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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

#### 8.6. 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

### 8.7. Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it 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 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

### 8.8. Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

### 8.9. Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

#### *Clause 9*

#### *Use of sub-processors*

N/A

#### *Clause 10*

#### *Data subject rights*

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate



such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lay down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

## *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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.
- (c) 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.
- (d) The Parties agree that if one Party is held liable under paragraph (c), 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.
- (e) The data importer may not invoke the conduct of a processor or 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.

#### *Clause 14*

##### *Local laws and practices affecting compliance with the Clauses*

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

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## Clause 15

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

#### **15.1. Notification**

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

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

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

(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.

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

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

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

### *Clause 17*

#### *Governing law*

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

### *Clause 18*

#### *Choice of forum and jurisdiction*

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

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

- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.



## ANNEX I

### A. LIST OF PARTIES

The contents of Section A of Schedule 1 are incorporated herein.

### B. DESCRIPTION OF TRANSFER

The contents of Section B Schedule 1 are incorporated herein.

### C. COMPETENT SUPERVISORY AUTHORITY

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

The Irish Data Protection Commission will be the competent supervisory authority.

## ANNEX II

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.*

See Schedule 2 for description of technical and organisational measures.

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.*

All Authorized Sub-Processors are required to implement and maintain the same or substantially similar technical and organizational measures, responsibilities and obligations as those required of the Processor under this DPA.

## Schedule 5

### UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Version B1.0, in force 21 March 2022

## Part 1: Tables

**Table 1: Parties**

Start date	Date of the executed Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: [INSERT] Trading name (if different): [INSERT] Main address (if a company registered address): [INSERT] Official registration number (if any) (company number or similar identifier): [INSERT]	Full legal name: Workato, Inc. Trading name (if different): N/A Main address (if a company registered address): 215 Castro St, Suite 300, Mountain View, CA94041 Official registration number (if any) (company number or similar identifier): 5451068
Key Contact	Full Name (optional): [INSERT] Job Title: [INSERT] Contact details including email: [INSERT]	Full Name (optional): [INSERT] Job Title: Chief Information Security Officer Contact details including email: privacy@workato.com
Signature (if required for the purposes of Section 2)		

**Table 2: Selected SCCs, Modules and Selected Clauses**

Addendum EU SCCs	<input type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: [INSERT] Reference (if any): [INSERT] Other identifier (if any): [INSERT] Or <input checked="" type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	One	Omitted	Omitted			

2	Two	Omitted	Omitted	X		
3						
4						

**Table 3: Appendix Information**

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Account Holder and Workato, Inc.
Annex 1B: Description of Transfer: See Schedule 1
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 2
Annex III: List of Sub processors (Modules 2 and 3 only): See <a href="https://www.workato.com/legal/sub-processors">https://www.workato.com/legal/sub-processors</a>

**Table 4: Ending this Addendum when the approved Addendum Changes**

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
---	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

- Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
----------	---

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

### Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

## Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
  - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
  - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
  - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section , the provisions of Section will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section ) are made:
  - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
  - b. In Clause 2, delete the words:
 

"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";
  - c. Clause 6 (Description of the transfer(s)) is replaced with:
 

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
  - d. Clause 8.7(i) of Module 1 is replaced with:
 

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
  - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
 

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
  - f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
  - g. References to Regulation (EU) 2018/1725 are removed;
  - h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
  - i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:
 

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
- m. Clause 17 is replaced with:
 

“These Clauses are governed by the laws of England and Wales.”;
- n. Clause 18 is replaced with:
 

“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
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

#### **Amendments to this Addendum**

- 16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
- 17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved Addendum which:
  - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
  - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

- 19. If the ICO issues a revised Approved Addendum under Section , if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
  - a. its direct costs of performing its obligations under the Addendum; and/or
  - b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

- 20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.



**Alternative Part 2 Mandatory Clauses:**

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
-------------------	---