

## DATA PROCESSING AMENDMENT

This Data Processing Amendment ("**DPA**") is entered into between \_\_\_\_\_ (collectively, "**Customer**") on behalf of itself and Customer Subsidiaries, and Symphonic Source, Inc dba Cloudingo, a Texas corporation on behalf of itself and its affiliates with a principal place of business 4004 Beltline Road, Suite 120, Addison, TX 75001 (collectively, "**Vendor**"). This DPA forms part of the Master Subscription Agreement or other written or electronic agreement between Vendor and Customer for the purchase of online services from Vendor (identified either as "**Services**" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data. Either of the parties to the DPA may be referred to as a "**Party**" or collectively as the "**Parties**."

### RECITALS

- A. Vendor has entered into one or more purchase orders, contracts and/or agreements (the "**Contract(s)**") with Customer and/or Customer Subsidiaries. In delivering the Services under the Contract(s), Vendor may process Personal Data controlled by Customer, a Customer Subsidiary and/or their respective customers, contacts or partners.
- B. As part of its privacy policy and its contractual arrangements and in order to comply with applicable law, Customer has provided certain assurances to its customers, contacts, partners and/or end-users to ensure the appropriate protection of Personal Data when Customer engages third party suppliers. Customer's engagement of Vendor is conditioned upon Vendor's agreement to the terms and conditions of this DPA.

### AGREEMENT

#### 1. DEFINITIONS

---

- 1.1 "**Applicable Privacy Law(s)**" means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, EU Data Protection Law, UK Data Protection Law, the FADP, and the CCPA.
- 1.2 "**Authorized Persons**" means any person who processes Personal Data on Vendor's behalf, including Vendor's employees, officers, partners, principals, contractors and sub-processors.
- 1.3 "**Customer Subsidiary**", "**Customer Subsidiaries**" means any entity that Customer controls (directly or indirectly), or is under common control, where "control" means at least fifty percent (50%) ownership of the outstanding shares of the entity, or the ability to direct the management of the entity by contract or otherwise.
- 1.4 "**EEA**" means the member states of the European Union and Iceland, Liechtenstein, and Norway.
- 1.5 "**EU Data Protection Law**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**").
- 1.6 "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations, including any amendments made by the California Privacy Rights and Enforcement Act ("CPRA").
- 1.7 The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Processor**," and "**Processing**," have the meanings given to them in Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given in EU Data Protection Law will apply.

- 1.8 “**FADP**” shall mean the Swiss Ordinance to the Federal Act on Data Protection and any revisions thereto.
- 1.9 “**Symphonic Source Affiliate**”, “**Symphonic Source Affiliates**” means any entity that Symphonic Source controls (directly or indirectly), where “control” means at least fifty percent (50%) ownership of the outstanding shares of the entity, or the ability to direct the management of the entity by contract or otherwise.
- 1.10 “**UK**” shall mean the United Kingdom.
- 1.11 “**UK Data Protection Law**” means the United Kingdom’s General Data Protection Regulations as implemented by the UK Data Protection Act of 2018 (“**UK GDPR**”).

## **2. ROLE AND SCOPE OF PROCESSING**

---

- 2.1 Vendor shall process Personal Data under the Contract(s) only as a Processor acting on behalf of Customer (whether as Controller or itself a Processor on behalf of third party Controllers).
- 2.2 Vendor will at all times: (i) process the Personal Data only for the purpose of providing the Services to Customer under the Contract(s) and in accordance with Customer's documented instructions (except where otherwise required by applicable law); (ii) not process the Personal Data for its own purposes or those of any third party, and (iii) not sell or share (as those terms are defined in the CCPA) Personal Data.
- 2.1 Vendor will at all times provide an adequate level of protection for the Personal Data as described in **Annex A**, wherever processed, in accordance with the requirements of Applicable Privacy Laws.

## **3. SUBPROCESSING**

---

- 3.1 Vendor shall not subcontract any processing of the Personal Data to a subcontractor without the prior written consent of Customer. Notwithstanding this, Customer consents to Vendor engaging subcontractors to process the Personal Data provided that:
- (a) Vendor provides at least 30 days prior written notice to Customer of the engagement of any new subcontractor (including details of the processing and location) and Vendor shall update the list of all subcontractors engaged to process Personal Data under this Agreement at **Annex B** and send such updated version to Customer prior to the engagement of the subcontractor;
  - (b) Vendor imposes substantially similar data protection terms on any subcontractor it engages as contained in this DPA (including the data security provisions in **Annex A** as well as any other applicable Annex to this Agreement); and
  - (c) Vendor remains fully liable for any breach of this DPA or the Contract(s) that is caused by an act, error or omission of such subcontractor.
- 3.2 If Customer objects to the engagement of any subcontractor on data protection grounds, then either Vendor will not engage the subcontractor to process the Personal Data or Customer may elect to suspend or terminate the processing of Personal Data under the Contract(s) without penalty.

## **4. COOPERATION**

---

- 4.1 Vendor shall reasonably cooperate to enable Customer to respond to any requests, complaints or other communications from data subjects and regulatory or judicial bodies relating to the processing

of Personal Data under the Contract(s), including requests from data subjects seeking to exercise their rights under Applicable Privacy Laws. In the event that any such request, complaint or communication is made directly to Vendor, Vendor shall promptly pass this onto Customer and shall not respond to such communication without Customer's express authorization.

- 4.2 If Vendor receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Personal Data, Vendor shall not disclose any information but shall immediately notify Customer in writing of such request, and reasonably cooperate with Customer if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.
- 4.4 To the extent Vendor is required by GDPR, UK GDPR, and/or FADP, Vendor will assist Customer (or its third party Controller) to comply with, as applicable, Articles 35 & 36 GDPR and Sections 64 and 65 of the UK GDPR; in particular, it will promptly notify Customer if it believes that its processing of Personal Data is likely to result in a high risk to the privacy rights of data subjects, and upon reasonable request, will assist Customer (or the relevant Controller) to carry out data protection impact assessments and for the relevant Controller to consult where necessary with data protection authorities.

## **5. EXPORT OF DATA ORIGINATING FROM EEA, SWITZERLAND, UK**

---

- 5.1 Where Vendor processes Personal Data under this DPA that originates from the EEA, Switzerland, and/or the UK, the Parties agree to the Standard Contractual Clauses for Processors ("**Standard Contractual Clauses**") attached hereto as **Annex D** and incorporated by reference to this DPA. Where the data originates from Switzerland, the Parties agree to amend the Standard Contractual Clauses as set forth in the Switzerland Data Processing Addendum attached hereto as **Annex E**. Where the data originates from the UK, the Parties agree to amend the Standard Contractual Clauses as set forth in the UK Data Processing Addendum attached hereto as **Annex F**.
- 5.2 It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail. In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.
- 5.3 Vendor acknowledges that Customer may disclose this DPA to the US Department of Commerce, the Federal Trade Commission, a European data protection authority, or any Swiss, US, UK or EU judicial or regulatory body upon their lawful request.

## **6. DELETION & RETURN**

---

- 6.1 Upon Customer's request, or upon termination or expiry of this DPA, Vendor shall destroy or return to Customer all Personal Data (including copies) in its possession or control (including any Personal Data processed by its subcontractors). This requirement shall not apply to the extent that Vendor is required by any applicable law to retain some or all of the Personal Data, in which event Vendor shall isolate and protect the Personal Data from any further processing except to the extent required by such law.


## **7. GENERAL**

---

- 7.1 The obligations placed upon the Vendor under this DPA shall survive so long as Vendor and/or its subcontractors processes Personal Data on behalf of Customer.

- 7.2 In the event there is any act or omission on the part of the Vendor and/or its Subcontractors which leads to Customer being liable for breaches of the GDPR or any third party contract, then Vendor shall indemnify Customer for any damage, loss, liabilities, costs, harm or expenses (including reasonable legal fees) suffered by Customer as a result.
- 7.3 This DPA may not be modified except by a subsequent written instrument signed by both parties.
- 7.4 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.
- 7.5 In the event of any conflict between this DPA and any data privacy provisions set out in any Contracts the parties agree that the terms of this DPA shall prevail.
- 7.6 Limitation of Liability. Symphonic Source and all its Symphonic Source Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Customer and Symphonic Source, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Master Subscription Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Master Subscription Agreement and all DPAs together. For the avoidance of doubt, Symphonic Source and Symphonic Source Affiliates' total liability for all claims from Customer and all of its Customer Subsidiaries arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Master Subscription Agreement, including by Customer and all Customer Subsidiaries, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Customer Subsidiary that is a contractual party to any such DPA. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules, Appendices, Annex.

By signing below, each party acknowledges that it has read and understood the terms of this DPA and agrees to be bound by them.

SYMPHONIC SOURCE, INC. (PROCESSOR)	CUSTOMER (CONTROLLER)
<p>DocuSigned by:    <small>A185905E19B24DD...</small></p> <p>By: _____</p> <p>Name: <u>Lars Nielsen</u></p> <p>Title: <u>President</u></p> <p>Date: <u>4/5/2023</u></p>	<p>By: _____</p> <p>Name: _____</p> <p>Title: _____</p> <p>Effective Date: _____</p>

## ANNEX A

### DATA SECURITY

1. Security Measures. Vendor will implement and maintain all appropriate technical and organizational security measures to protect from Security Incidents and to preserve the security, integrity and confidentiality of Personal Data ("**Security Measures**"). Such measures shall have regard to 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. At a minimum, Vendor agrees to the Security Measures identified in this Annex A.
2. Data Security. Vendor has established and shall maintain during the Term an information security program that meets or exceeds SOC 2 Type II compliance, Applicable Privacy Law(s), and all other applicable federal, state and local laws, regulations and best practices as well as all applicable laws and regulations in the jurisdiction(s) that Vendor transmits, processes, and stores Customer Confidential Information, including administrative, technical and physical safeguards designed to: (i) protect the security, confidentiality and integrity of Customer Confidential Information; (ii) protect against anticipated threats or hazards to the security, confidentiality and integrity of Customer Confidential Information; (iii) protect against unauthorized access to or use of Customer Confidential Information; (iv) ensure compliance with an active incident response program; and (v) ensure the proper disposal of Customer Confidential Information. Vendor shall provide Customer with a copy of its information security program and policies upon Customer's request.
3. Security Incident; Response. The term "*Security Incident*" means (i) any actual, attempted or suspected unauthorized access to, or acquisition or use of any Customer Confidential Information or Customer Data, or any other occurrence which may compromise the availability, security, or confidentiality of Customer, Customer Confidential Information, Customer Data, or Customer's infrastructure or operations; or (ii) of any disclosure, intended, accidental or otherwise, wherein Customer Confidential Information or Customer Data is, or was, accessed or acquired by an unauthorized person or accessed or used in an unauthorized manner; (iii) any other event that compromises the security, confidentiality or integrity of Customer Confidential Information; or (ii) Vendor's breach of any of its obligations related to the security and privacy of Customer Confidential Information, Customer Data, or Customer under this Agreement or any other obligation that triggers a related disclosure requirement under applicable law, regulation or agreement. In the event of a Security Incident, the Parties shall proceed as follows:
4. Notification to Customer. Vendor shall notify Customer in writing and by the most expedient of means of any Security Incident in the most expedient time possible and, in no event, more than twenty-four (24) hours after the suspicion, discovery or notification of a Security Incident (each, a "*Security Incident Notification*").
5. Additional Notifications. Excluding a Security Incident Notification, the content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at Customer's discretion, except as otherwise required by applicable laws.
6. Content of Security Incident Notification. The Security Incident Notification shall be written and include to the extent known: (i) a detailed description of the Security Incident; (ii) all known details of the Security Incident, including what data, information, or Customer Infrastructure is impacted; (iii) the identity of each affected person; (iv) measures taken by Vendor to identify, prevent and mitigate the effects of the Security Incident; and (v) any other relevant information and documentation that Customer may request concerning the Security Incident. Vendor shall provide Customer with written updates to the Security Incident Notification on a daily basis (or at a different interval set by Customer) until the Security Incident has been resolved. The Vendor is responsible for updating this notification to Customer routinely and timely as information about the Security Incident emerges.
7. Vendor Remedial Action. Upon discovery or notification of a Security Incident, and subject to Section 9 (Limitation on Disclosure) of this Annex, Vendor shall take immediate action, at its own expense and in compliance with applicable law, to: (i) investigate the Security Incident; (ii) identify, prevent and mitigate the effects of the Security Incident; (iii) perform all other actions reasonably

necessary to remedy the Security Incident, prevent future incidents of the same or similar nature, and to otherwise restore the confidentiality, security and integrity of Customer, including Customer Confidential Information in Vendor's possession, custody, or control; and (iv) perform those actions and provide the support reasonably requested by Customer. Vendor shall pay for or reimburse Customer for all damages, costs, losses, fines, penalties and expenses related to a Security Incident including, but not limited to, those incurred by Customer in connection with preparing and providing notice to impacted data subjects, as well as other related support services such as credit monitoring services and call center services, and regulatory or other governmental fines.

8. Compliance Audits. Customer (or its appointed representatives) may carry out an inspection of Vendor's operations and facilities during normal business hours and subject to reasonable prior notice where Customer considers it necessary or appropriate (for example, without limitation, where Customer has reasonable concerns about Vendor's data protection compliance, following a Security Incident or following instruction from a data protection authority).
9. Limitation on Disclosure. Unless otherwise required or prohibited by law, Vendor shall not disclose to any third party the occurrence of, or any information relating to, a Security Incident without Customer's prior written approval.
10. Full Cooperation. Vendor shall fully cooperate with Customer in connection with its efforts regarding the Security Incident. Such cooperation shall include, but not be limited to, the provision of all requested access to software, systems and facilities under Vendor's control and the immediate provision of all requested information relevant to its efforts.
11. Data Access. Vendor shall ensure that any Authorized Person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for the purpose of delivering the Services under the Contract(s) to Customer.

**List of Vendor's Subcontractors**

**[List all Subcontractors here (including any and all Vendor affiliates processing Personal Data).]**

<b>Name</b>	<b>Nature of Processing</b>	<b>Territory(ies)</b>
<b>IBM</b>	<b>Private Cloud Hosting, physical infrastructure</b>	<b>Dallas, TX</b>

ANNEX C

INFORMATION FOR PROCESSING OF DATA SUBJECT TO STANDARD CONTRACTUAL CLAUSES

I. List of Parties

Data Exporter:

Name: \_\_\_\_\_ (“Customer”)

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

Official registration number (if any) (company number or similar identifier):

Customer Contact Information:

- Name:
- Position:
- Email:
- Data Protection Officer (if applicable):
- Representative in the EU (if applicable):

Activities relevant to the data transferred under these Clauses:

Symphonic Source provides the Cloudingo software which can be used to remove Salesforce data duplicates for Customer. Cloudingo indexes records in Salesforce and facilitates the merging of records deemed to contain duplicated or similar data (specifically the Lead, Contact, Account objects inside Salesforce).

Signature and date: .....

Role: Controller

Data Importer(s):

Name: Symphonic Source, Inc.

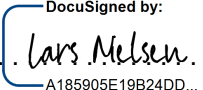
Address: 4004 Beltline Road, Suite 120, Addison, TX 75001

Contact Responsible for Data Protection:

- Name: Lars Nielsen
- Position: President
- Email: lars.nielsen@cloudingo.com

Activities relevant to the data transferred under these Clauses:

Symphonic Source provides the Cloudingo software which can be used to remove Salesforce data duplicates for Customer. Cloudingo indexes records in Salesforce and facilitates the merging of records deemed to contain duplicated or similar data (specifically the Lead, Contact, Account objects inside Salesforce).

Signature and date: . . .  . . . 4/5/2023 . . .

DocuSigned by:  
A185905E19B24DD...

Role: Processor



## **II. Description of Transfer**

### **1. Categories of data subjects whose personal data is transferred (controlled by Customer in its sole discretion, and which may include, but is not limited to the following)**

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Services

### **2. Categories of personal data transferred (controlled by Customer in its sole discretion, and which may include, but is not limited to the following)**

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Localisation data

### **3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. For reference, Sensitive Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.**

The Customer does not expect to provide Sensitive Data to Vendor. Applied restrictions and safeguards for the processing of the data are included in Annex A.

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

Continuous during the provision of the Services to Customer.

### **5. Nature of the processing.**

Symphonic Source will process the data using its Cloudingo software to remove Salesforce data duplicates for Customer. Cloudingo indexes records in Salesforce and facilitates the merging of records deemed to contain duplicated or similar data (specifically the Lead, Contact, Account objects inside Salesforce).

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

Listed above in No. 5.

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

Vendor will retain the data for the duration of the Agreement subject to Section 6 of the DPA.

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

As stated above.

## ANNEX D

### STANDARD CONTRACTUAL CLAUSES

Controller to Processor

#### SECTION I

##### *Clause 1*

##### **Purpose and scope**

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

have agreed to these standard contractual clauses (hereinafter: 'Clauses') as set forth in their Data Processing Agreement.

- (c) These Clauses apply with respect to the transfer of personal data as specified in the Data Processing Agreement and Annex C.II.
- (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 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### **Clause 4**

#### **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### **Clause 5**

#### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### **Clause 6**

#### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex C.II.

### **Clause 7**

## **Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex C.I.
- (b) Once it has completed the Appendix and signed Annex C.I., the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex C.I.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **SECTION II – OBLIGATIONS OF THE PARTIES**

### *Clause 8*

#### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex C.II., 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 A and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

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

### **8.5 Duration of processing and erasure or return of data**

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

### **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex B. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach.

Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

### **8.7 Sensitive data**

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

### **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 <sup>(1)</sup> (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.

---

<sup>1</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

## **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 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex B. The Parties shall keep Annex B up to date.
- (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. <sup>(2)</sup> 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.

---

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



- (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 A the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

## ***Clause 11***

### **Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
- (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## ***Clause 12***

### **Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13**

#### **Supervision**

- (a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer 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 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: German Federal Commissioner for Data Protection and Freedom of Information.

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

## ***Clause 15***

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

#### **15.1 Notification**

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

- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV – FINAL PROVISIONS**

### ***Clause 16***

#### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### ***Clause 17***

#### **Governing law**

These Clauses shall be governed by the law of 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 Germany.

### ***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 Germany.
- (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 E

### SWITZERLAND DATA PROCESSING ADDENDUM

This Switzerland Data Processing Addendum (“**Swiss Addendum**”) is entered into by the parties as set forth in the attached Data Processing Agreement. This Swiss Addendum modifies and amends the Standard Contractual Clauses in Annex D (the “**SCCs**”) in accordance with to the Swiss Ordinance to the Federal Act on Data Protection (“**FADP**”).

1. If the data transmission is exclusively subject to the FADP, the Competent Supervisory Authority in Clause 13 of the shall be designated as the Swiss Federal Data Protection and Information Commissioner (“**FDPIC**”). If the data transmission is subject to both the FADP and the GDPR, the Competent Supervisory Authority in Clause 13 shall be designated as the FDPIC in addition to the authority designated in Clause 13.
2. The term “member state” in the SCCs is not to be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence.
3. References to the GSPR in the SCCs shall also be understood as references to the FADP as appropriate for data exports or other data processing activities that are covered by the FADP.
4. The clauses of the SCCs also protect the data of legal entities until entry into force of the revised FADP scheduled to come into force on January 1, 2023.



## Annex F

### UK DATA PROCESSING ADDENDUM

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## Part 1: Tables

**Table 1: Parties**

<b>Start date</b>	Last Signature Date in Data Processing Agreement, Annex C.	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	Identified in Data Processing Agreement, Annex C.	Identified in Data Processing Agreement, Annex C.
<b>Key Contact</b>	Identified in Data Processing Agreement, Annex C.	Identified in Data Processing Agreement, Annex C.
<b>Signature (if required for the purposes of Section 2)</b>	Not required. The parties enter into this addendum by signing the Data Processing Agreement.	Not required. The parties enter into this addendum by signing the Data Processing Agreement.

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

<b>Addendum EU SCCs</b>	<p>1. <input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: 4.6.2021</p> <p>Reference (if any): C(2021) 3972 final</p> <p>Other identifier (if any): [REDACTED]</p> <p>Or</p> <p>2. <input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules,</p>
-------------------------	---

		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	N/A	N/A	N/A	N/A	N/A	N/A
2						
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: **Provided in DPA Annex C**

Annex 1B: Description of Transfer: **Provided in DPA Annex C**

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: **Provided in DPA Annex A**

Annex III: List of Sub processors (Modules 2 and 3 only): **Provided in DPA Annex B**

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

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

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. 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.
2. 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

3. 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 10 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 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) 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 18, 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.