# DATA PROCESSING TERMS FOR SUPPLIERS

If these Data Processing Terms ("**Data Processing Terms**") are expressly incorporated by reference into an Agreement between Sophos and Supplier, these Data Processing Terms form part of the Agreement between Supplier and Sophos where the supply of the Services involves the Processing of Sophos Data.

**BACKGROUND:**

(A) Sophos processes Personal Data (as defined below) in connection with their business activities.
(B) Sophos wishes to receive, and Supplier wishes to provide the Services under existing and/or future agreement(s) between the parties ("**Agreement**").
(C) Supplier may process Sophos Data as a consequence of the Agreement.
(D) The Data Protection Laws and Regulations provide that such Processing (as defined below) shall be governed by an agreement.
(E) The parties wish to be bound by these Data Processing Terms to satisfy such requirement.

## 1. DEFINITIONS

1.1 In these Data Processing Terms, the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

**"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the ICO as set out at Exhibit 5 attached hereto;

**"Affiliate"** means a company that, directly or indirectly, controls, is controlled by or is under common control with the subject entity. "**Control**," for the purposes of this definition, means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity;

**"Appropriate Technical and Organisational Measures", "Controller", "Processor", "Data Subject", "Personal Data", "Processing"** and **"Supervisory Authority"** shall be interpreted in accordance with the GDPR;

"**CCPA**" means the California Consumer Privacy Act;

"**Clauses**" shall have the meaning ascribed to it in the EU SCCs;

"**Customers**" means customers of Sophos;

**"Data Protection Laws and Regulations"** means all laws and regulations, including laws in the EEA, the European Union, the United Kingdom, Switzerland and the United States (including, but not limited to, the CCPA) and its respective states, applicable to the Processing of Personal Data under this Agreement;

"**EEA**" means the European Economic Area;

"**EU SCCs**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by the European Commission implementing decision (EU) 2021/914 of 4 June 2021;

**"GDPR"** means the General Data Protection Regulation (EU) 2016/679;

"**ICO**" means The Information Commissioner's Office established in the United Kingdom.

"**Measures**" means the technical and organisational measures set out in Exhibit 3 attached hereto;

"**Personnel**" means the officers, directors, contractors and employees of the Supplier;

**"Services"** means the services provided by the Supplier to Sophos under the terms of the Agreement;

**"Sophos"** means the entity within the Sophos group of companies that is the Sophos contracting party to the Agreement, acting for itself and for and on behalf of its Affiliates and Customers;

"**Sophos Data**" means any and all Personal Data which the Supplier processes (i) as a Processor on behalf of Sophos as the Controller, and (ii) as a sub-processor on behalf of Sophos as the Processor in cases where Customers are the Controllers and which is subject to the Data Protection Laws and Regulations;

"**SOW**" means a statement of work entered into between Sophos and Supplier in relation to the Agreement.

**"Supplier**" means the provider of the Services as set out in the Agreement;

## 2. SUPPLIER OBLIGATIONS

2.1 Supplier agrees that Sophos and its Customers located in the EEA, the United Kingdom and Switzerland, are the Controllers and Supplier is the Processor or sub-processor in relation to the Sophos Data. The nature and purpose of the Processing, the types of Sophos Data which Supplier processes and the categories of Data Subjects whose Sophos Data is processed are set out in Exhibit 2 attached hereto.

2.2 Supplier shall:

2.2.1 comply with the Data Protection Laws and Regulations;

2.2.2 process Sophos Data only in compliance with Sophos' written instructions (which may be specific instructions or instructions of a general nature as set out in a SOW, the Agreement or as communicated by Sophos in writing from time to time) and not for any other purpose. If Supplier is required to process the Sophos Data for any other purpose by law to which Supplier is subject, Supplier will inform Sophos of this requirement before the Processing, unless that law prohibits this t;

2.2.3 notify Sophos immediately in writing if, in Supplier's opinion, an instruction for the Processing of the Sophos Data given by Sophos infringes the Data Protection Laws and Regulations;

2.2.4 taking into account the nature of the Processing, assist Sophos:

2.2.4.1 by implementing the Measures and in so far as it is possible, in fulfilling Sophos's obligations to respond to requests from Data Subjects exercising their rights under the Data Protection Laws and Regulations; and

2.2.4.2 in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR or equivalent provisions in the Data Protection Laws and Regulations;

2.2.5 implement and maintain the Measures to protect the Sophos Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, access, theft, alteration or disclosure. These Measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction, damage, access or theft of the Sophos Data and having regard to the nature of the Sophos Data which is to be protected. As a minimum, these shall include the requirements required under (i) the Data Protection Laws and Regulations, and (ii) Exhibit 3 attached hereto. The Supplier may change or amend the Measures without the prior written consent of Sophos provided that the amended Measures maintain at least an equivalent level of protection and are notified to Sophos within [20] days of being changed or amended. Sophos may ask Supplier at any time to provide, within a reasonable timescale, a written description of the Measures Supplier employs for Processing Sophos Data and Sophos may make the same available to third parties;

2.2.6 take reasonable steps to ensure the reliability and competence of Supplier Personnel who have access to the Sophos Data;

2.2.7 ensure that Personnel required to access the Sophos Data are informed of the

confidential nature of the Sophos Data and comply with the obligations set out in these Data Processing Terms;

2.2.8 ensure that none of Supplier's Personnel publish, disclose or divulge any of the Sophos Data to any third party other than in accordance with these Data Processing Terms;

2.2.9 allow Sophos and its respective auditors or authorised agents to conduct audits or inspections during the term of the Agreement, which will include providing access to the Supplier's premises, resources, the Personnel and Supplier's Sub-Processors used in the provision of the Services and provide all reasonable assistance to Sophos in exercising its audit rights under these Data Processing Terms. The purposes of an audit pursuant to these Data Processing Terms includes, but is not limited to, verifying that Supplier is Processing the Sophos Data in accordance with Supplier's obligations under these Data Processing Terms, the Agreement and applicable Data Protection Laws and Regulations;

2.2.10 not retain or process any Sophos Data for longer than is necessary to perform their obligations under the Agreement or applicable SOW, and at the end of the provision of the Services or upon Sophos' written request, return or securely destroy such Sophos Data. Supplier shall provide Sophos with written certification of the destruction of the Sophos Data; and

2.2.11 process Sophos Data at the locations agreed upon in the Agreement or applicable SOW and shall not transfer Sophos Data across country borders unless expressly authorised in writing by Sophos and such transfers shall be in accordance with clause 9 below.

2.3 The Supplier shall not sell Sophos Data.

**3. BREACH NOTIFICATION**

3.1 In the event of any actual or reasonably suspected, accidental or unauthorised access, use, disclosure, tampering, alteration, destruction or loss of Personal Data ("**Data Breach**"), Supplier will notify dataprotection@sophos.com and security@sophos.com no later than forty-eight (48) hours after the initial discovery of such Data Breach. Supplier shall promptly provide all information and assistance that Sophos requires in the investigation, mitigation, notification, and remediation of such Data Breach and shall provide Sophos (or an independent third party designated by Sophos) with access to its premises and systems for the purposes of investigating the Data Breach in accordance with clause 2.2.9 above, upon forty-eight (48) hours' advance notice from Sophos.

3.2 Supplier shall not, unless instructed to do so in writing by Sophos, notify Data Subjects or regulatory authorities of a Data Breach, and Supplier will take such steps (i) as deemed necessary by Sophos, and (ii) as legally required under applicable law, to protect affected Data Subjects from fraud or identity theft and any other damage in each case as is necessary including, but not limited to, reimbursing Sophos and holding it harmless for any cost related to notifications and, where applicable in accordance with the Data Protection Laws and Regulations, for the costs of providing credit reporting and/or monitoring services for Data Subjects actually or potentially affected by a Data Breach.

**4. PERSONNEL**

Supplier shall inform and regularly train its Personnel who are responsible for handling and protecting Sophos Data about privacy laws and regulations, and about the obligation to protect Sophos Data in accordance with the requirements of these Data Processing Terms.

**5. SUBPROCESSORS**

5.1 The Supplier has Sophos' general authorisation for the engagement of a third party (including, but not limited, any Supplier Affiliates, group companies or sub-contractors) ("**Sub-Processor(s)**") that Sophos has been notified of by Supplier at the time of execution of the Agreement. Supplier shall specifically inform Sophos in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving Sophos sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). Supplier shall provide Sophos with the information necessary to enable the data exporter to exercise its right to object. Notwithstanding the foregoing authorization, Supplier

must:

5.1.1 ensure the reliability and competence of the Sub-Processor, its employees and agents who may have access to the Sophos Data; and

5.1.2 enter into a written contract with the Sub-Processor, which includes provisions substantially similar to, and which are no less onerous than, these Data Processing Terms and as are required by the Data Protection Laws and Regulations.

5.2 For the avoidance of doubt, where a Sub-Processor fails to fulfil its obligations under any sub-processing contract or the Data Protection Laws and Regulations, Supplier will remain fully liable to Sophos for the fulfilment of Supplier's obligations under these Data Processing Terms, the Agreement and the Data Protection Laws and Regulations.

5.3 If the Supplier processes Personal Data of Canadian residents subject to the provisions of the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), then the Supplier shall:

5.3.1 ensure that the Sub-Processors are third parties under PIPEDA; and

5.3.2 conduct appropriate due diligence on its Sub-Processors.

## 6. LIMITATION OF LIABILITY

6.1 The Supplier will indemnify Sophos from and against any and all fines, losses, and/or damages incurred by Sophos and (if applicable) Customers, as a result of the Supplier's breach of these Data Processing Terms or the Data Protection Laws and Regulations.

6.2 The Supplier's liability to Sophos under these Data Processing Terms shall not exceed the greater of:

6.2.1 any limitation or exclusion of liability which applies to the Supplier as set forth in the Agreement; or

6.2.2 the sum of five million dollars (US$5,000,000.00) per claim.

## 7. CONFLICTS

In the event of any conflict or inconsistency between the provisions of the Agreement and these Data Processing Terms, the provisions of these Data Processing Terms shall prevail to the extent that they are more stringent than those in the Agreement, unless such provisions are expressly and specifically stated to have been amended by a provision in the Agreement or relevant SOW.

## 8. DURATION

The Processing will be carried out by the Supplier until the later of (i) the date that Supplier ceases to provide the Services to Sophos, (ii) the date the Supplier deletes or returns the Personal Data to Sophos, or (iii) the date that the Supplier ceases Processing Sophos Data.

## 9. TRANSFERS OF SOPHOS DATA

9.1 If the European Commission lays down, or an applicable supervisory authority adopts, standard contractual clauses for the matters referred to in Article 28(3) and Article 28(4) of the GDPR pursuant to Article 28(7) or Article 28(8) of the GDPR (as appropriate) and Sophos notifies Supplier that it wishes to incorporate any element of any such standard contractual clauses into the Agreement, Supplier will agree to the changes as reasonably required by Sophos to achieve this.

9.2 Supplier will not process Sophos Data outside the EEA or the UK, or in a country in respect of which a valid adequacy decision has not been issued by the European Commission or the ICO that is applicable to the Sophos Data being Processed, except with the prior written consent of Sophos as set out in these Data Processing Terms. Subject to clause 9.5, such transfers will be made subject to the terms of the EU SCCs (which are deemed incorporated into and form part of

this DPA), or any replacement or additional form of safeguard approved by the European Commission or as applicable in the UK, Switzerland or Jersey.

9.3 If either the European Commission or the ICO decision authorising the data transfer mechanism used to legitimise the transfers of Personal Data made under the Agreement is held to be invalid, or any supervisory authority requires transfers of Personal Data made pursuant to such decision to be suspended, then Sophos may, at its discretion, require Supplier to cease Processing Sophos Data to which this clause applies immediately, or promptly co-operate with Sophos to facilitate use of an alternative transfer mechanism.

9.4 Upon request, Supplier shall evidence to Sophos that EU SCCs (or the equivalent safeguard applicable in the UK, Switzerland or Jersey) are in place with data importers in third countries that are Processing Sophos Data.

9.5 The parties agree that transfers of Sophos Data from the UK to a third country or international organisation not benefitting from an adequacy decision under Article 45 of the GDPR (as it applies under English law) will be subject to the EU SCCs as amended by the UK Addendum, as may be amended or superseded from time to time.

9.6 For each Module to the EU SCCs, where applicable:

9.6.1 the details indicated in Exhibit 4 attached hereto shall be used;

9.6.2 the optional docking clause in Clause 7 shall not apply;

9.6.3 Option 1 under Clause 9 shall apply. The data importer shall notify the data exporter 30 days in advance of any intended changes (via addition or replacement) to the list of sub-processors listed in Exhibit 1.

9.6.4 in Clause 11, the optional language shall not apply;

9.6.5 For the purposes of Clauses 13(a):

9.6.5.1 where the data exporter is established in an EU Member State: The competent supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 with regards to the data transfer will be the competent supervisory authority where the data exporter is established.

9.6.5.2 Where the data exporter is established in the UK, the ICO shall act as the competent supervisory authority

9.6.6 For the purposes of Clause 17, the EU SCC's shall be governed by the law of the EU Member State in which the data exporter is established;

9.6.7 For the purposes of Clause 18(b), disputes will be resolved before the courts of the EU member state in which the data exporter is established.

9.7 Supplier will enter into the Module of EU SCCs selected by Sophos and shall promptly assist Sophos with the completion of the EU SCCs, including any addendum thereto.

**10 GENERAL**

10.1 Sophos and any Sophos Affiliate shall be a beneficiary of these Data Processing Terms.

10.2 Unless a separate Data Processing Agreement has been signed between the parties, these Data Processing Terms shall constitute the entire agreement between the parties in relation to Personal Data collected, processed and used by the Supplier on behalf of Sophos, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of the subject of Personal Data handling.

10.3 These Data Processing Terms shall be governed by and construed in accordance with the laws of

England and Wales and the English courts shall have exclusive jurisdiction to determine any disputes which may arise out of, under, or in connection with these Data Processing Terms.

10.4 Without limitation of any other rights available in law or equity, Sophos may seek injunctive relief from any jurisdiction or venue if, in the sole discretion of the Sophos, such measures are deemed appropriate to protect Sophos Data.

10.5 A variation of these Data Processing Terms is valid only if it is in writing and signed on behalf of each party.

10.6 Any failure by either party in exercising its rights, powers, or privileges under these Data Processing Terms shall not act as a waiver, nor shall any single or partial exercise preclude any further exercise of a right, power, or privilege by that party.

10.7 In the event that any one (1) or more of the provisions of these Data Processing Terms shall for any reason be held to be invalid, illegal, or unenforceable, the remaining provisions of these Data Processing Terms shall continue in full force and effect and the parties will negotiate in good faith to substitute a provision of like effect and intent to that deemed to be unenforceable.

10.8 To the extent of any conflict with the provisions of these Data Processing Terms and the Clauses of any EU SCC's entered into by the parties, the Clauses of the applicable EU SCC's (including any addendums thereto), shall take precedence.

**LIST OF APPENDICES**

**Exhibit 1: LIST OF SUB-PROCESSORS**
**Exhibit 2: DETAILS OF PROCESSING**
**Exhibit 3: TECHNICAL AND ORGANISATIONAL MEASURES**
**Exhibit 4: REFERENCE DATA for EU SCC**
**Exhibit 5: UK ADDENDUM**

## Exhibit 1 - LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:
As notified by Supplier at the time of execution of the Agreement.

## Exhibit 2 - DETAILS OF THE PROCESSING

***1. Categories of data subjects whose personal data is transferred:***

The Personal Data concern the following categories of data subjects:
Sophos may submit certain Personal Data to be Processed by the Supplier, the extent of which is determined and controlled by Sophos in its sole discretion, and which may include, but is not limited to Personal Data relating to the individuals about whom data is provided to the Supplier via the Services by (or at the direction of) Sophos or Sophos' end users, such as but not limited to

- Prospects, customers, business partners and vendors of Sophos;
- Employees or contact persons of Sophos' prospective customers, customers, business partners and vendors; or
- Employees, agents, and contractors of Sophos

***2. Categories of personal data transferred:***

The Personal Data concern the following categories of data:
Sophos may submit Personal Data to be Processed by the Supplier, the extent of which is determined and controlled by Sophos in its sole discretion, and which may include, but is not limited to:

- First and last name;
- Contact information (company, email, ***phone***, physical business address);
- Employment details such as title, manager's name, salary and benefits; or
- Sophos employee beneficiary information

The Personal Data concern the following special categories of data:

- None

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

Continuous

***4. Nature of the processing:***

Providing the Services purchased by Sophos under and pursuant to the Agreement

***5. Purpose(s) of the data transfer and further processing:***

Supplier will process Personal Data as necessary to perform the Services pursuant to the Agreement and as instructed by Sophos in its use of the Services.

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

The Personal Data will be processed for the following duration:
Subject to clause 8 of the Data Processing Terms, Supplier will process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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

As set out in Exhibit 1 above**.**

## Exhibit 3 - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

### A. Organisational Controls

1) The Supplier shall maintain a data protection and information security policy.
2) All Supplier's employees and other individuals with access to Sophos data must be trained on (i) the importance of data protection and information security, (ii) the content of the Supplier's data protection and information security policy, (iii) the Supplier's data protection and information security controls, and (iv) each individual's responsibilities with respect to data protection and information security.
3) The Supplier shall appoint an individual with responsibility for data protection and information security.

### B. Business Continuity Measures

1) The Supplier must protect its premises from fire, flood and other environmental hazards.
2) Servers and other critical IT equipment shall be stored in climate-controlled data centres.
3) The Supplier will maintain back-up generators to maintain power supplies in the event of power outages.
4) The Supplier shall maintain a business continuity plan and shall provide a copy for review by Sophos upon request.
5) The Supplier shall test its business continuity plan at least once per annum and shall provide Sophos with the results upon request.

### C. Physical Controls

The Supplier shall maintain the following physical controls:

1) Fit appropriate locks or other physical controls to doors and windows;
2) Entry to the Supplier's premises shall be controlled by ID cards with PINs;
3) All visitors shall be required to report to Reception or Security upon arrival;
4) All visitors shall be accompanied by Supplier personnel at all times while on the Supplier's premises;
5) All servers shall be housed in locked cages or locked data rooms with limited access and CCTV surveillance;
6) Use removable media (such as removable hard-drives, CDs and USB sticks) only where essential for the performance of the Agreement;
7) Unattended laptops and removable media must be physically secured (for example by locking away);
8) Permanently and irreversibly erase data from laptops and removable media once the essential purpose has been fulfilled;
9) Permanently and irreversibly erase data from computer equipment before disposal.

### D. Testing and Change Control

1) The Supplier shall maintain and apply a change control process for the deployment of new hardware, software, systems and developments.
2) The Supplier shall test all new hardware, software, systems and developments prior to release to the production environment.
3) The production environment must be separate from test systems.
4) Sophos data may not be used on test systems or for any test purposes unless Sophos expressly agrees otherwise in writing.
5) The Supplier shall verify the success of the deployment into the production environment.

### E. Logical Controls

The Supplier shall maintain the following logical controls:

1) Firewalls and intrusion detection mechanisms;
2) Access control approval procedures to ensure that access is only granted to individuals that have an express need for the data;
3) Immediate removal of access rights for individuals that no longer require access or have ceased to be employed/engaged by Supplier;
4) System access and event logging;
5) Fully updated malware and spyware protection;
6) Individual user IDs and strong passwords which are changed at least every 30 days;
7) Encryption of laptops and other removable media;
8) Encryption of data when in transit and at rest;
9) Logical separation of Sophos data from data belonging to other customers;
10) Remote access must be restricted to authorized individuals via a secure virtual private network.

**Exhibit 4 – REFERENCE DATA FOR THE APPENDIX OF THE EU STANDARD CONTRACTUAL CLAUSES**

☒ **MODULE TWO: Transfer controller to processor shall apply**

**ANNEX I**

**A. LIST OF PARTIES**

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

| | |
|---|---|
| Name | Sophos Limited (for and on behalf of its EU and Swiss subsidiaries |
| Address | The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK |
| Other information needed to identify the Organisation | Registration number: 2096520 |
| Contact person's<br>Name:<br>Position:<br>Contact details: | <br><br>Privacy Counsel<br>dataprotection@sophos.com |
| Activities relevant to the data transferred under these Clauses | In accordance with the Agreement |
| Role | Controller |

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

| | |
|---|---|
| Name | As provided to Sophos under the Agreement |
| Address | As provided to Sophos under the Agreement |
| Contact person's<br>Name:<br>Position:<br>Contact details: | As provided to Sophos under the Agreement |
| Activities relevant to the data transferred under these Clauses | As described in Clause 2 above |
| Role | Processor |

**B. DESCRIPTION OF TRANSFER**

As set out in Exhibit 2 above

**C. COMPETENT SUPERVISORY AUTHORITY**

As set out in clause 9.6 of the Data Processing Terms

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

As set out in Exhibit 3 above

## ANNEX III – LIST OF SUB-PROCESSORS

Controller has chosen Clause 9 (a), Option 2 of the EU SCC.

The controller has authorised the use of the sub-processors as set out in clause 5 of the Data Processing Terms

**Exhibit 5 - UK ADDENDUM**

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

**VERSION B1.0, in force 21 March 2022**

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

| | | |
|---|---|---|
| **Start date** | Beginning of providing the Services under the Agreement | |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' details** | Full legal name: Sophos Limited (for and on behalf of its EU and Swiss subsidiaries<br>Registered address): The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK<br>Company number: 2096520 | As set out in Exhibit 4 above |
| **Key Contact** | Job Title: Privacy Counsel<br>Contact details including email: dataprotection@sophos.com | As set out in Exhibit 4 above |

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

| | |
|---|---|
| **Addendum EU SCCs** | 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? |
|---|---|---|---|---|---|---|
| **2** | 2 | Not applicable | Not applicable | As set out in clause 9.6 of the Data Processing Terms | As set out in clause 9.6 of the Data Processing Terms | no |

### 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: As set out in Exhibit 4 above |
| Annex 1B: Description of Transfer: As set out in Exhibit 4 above |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:<br>As set out in Exhibit 4 above |
| Annex III: List of Sub processors (Modules 2 and 3 only):<br>As set out in Exhibit 4 above |

### 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:<br>☐ Importer<br>☒ Exporter<br>☐ neither Party |

# 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 above. |
| **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.