

## VENDOR DATA PROCESSING ADDENDUM

### *Controller to Processor*

*Last revised 20 October 2022*

This Data Processing Addendum and all Annexes hereto (“DPA”) between SolarWinds Worldwide, LLC (“SolarWinds”) acting on its own behalf and as agent for each SolarWinds Affiliate, and the Vendor (“Vendor”).

This DPA forms part of the Vendor Agreement (“Agreement”), entered into between Vendor and SolarWinds, and applies to the extent that Vendor processes Personal Data on behalf of SolarWinds in the course of providing the Services.

This DPA serves as the final and entire expression of the parties’ agreement on the subject matter hereof, and is effective upon its incorporation into the Agreement.

For clarity, any terms capitalized and not defined here shall have the meaning as defined in the Agreement.

---

#### **HOW TO EXECUTE THIS DPA:**

1. This DPA consists of four parts: the DPA main body, the Standard Contractual Clauses (SCC) in Exhibit 1 (including Appendix), the UK Addendum in Exhibit 2, (UK data transfer purposes) Exhibit 3 (Swiss data transfer purposes) and Exhibit 4 (CCPA purposes).
2. To complete this DPA, You must:
  - a. Complete the information in the signature boxes on page 8.
  - b. Complete sub-processor information at Section 5.2 of page 4.
  - c. Complete information on pages 22 and 23.
  - d. Complete information at Table 3 of the UK Addendum on page 26.
  - e. Sign on pages 8 and 22.

## DATA PROCESSING TERMS

### 1. Definitions.

1.1 **Affiliate** means an entity that owns or controls, is owned or controlled by, or is or under common control or ownership with either SolarWinds or Vendor (as the context allows), where control is defined as the possession, directly or indirectly, or the power to direct or cause the direction of an entity's management and policies, whether through ownership of voting security, by contract, or otherwise;

1.2 **Controller** means the entity which determines the purposes and means of the Processing of Personal Data;

1.3 **Data Protection Laws** means to the extent applicable: (i) GDPR and any applicable national associated laws or implementations thereof; (ii) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance; (iii) GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("**UK GDPR**"), together with the Data Protection Act 2018 ("**UK Data Protection Law**"); and (iv) State Privacy Laws; in each case, as may be amended, supplemented or replaced from time to time.

1.4 **Data Security Incident** means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data;

1.5 **Data Subject** means the identified or identifiable person to whom Personal Data relates, and includes "consumer" as defined in CCPA;

1.6 **Data Subject Request** means a request from or on behalf of a Data Subject to exercise any right under relevant Data Protection Laws;

1.7 **EEA** means the European Economic Area and, unless otherwise indicated, as used in this DPA, "EEA" or "EEA Member States" includes the United Kingdom ("UK");

1.8 **GDPR** means the General Data Protection Regulation, 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, and repealing Directive 95/46/EC;

1.9 **Personal Data** means any information relating to an identified or identifiable natural person processed by Vendor on SolarWinds's behalf pursuant to the Agreement, and includes "personal information" as defined in CCPA;

1.10 **Processing** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.11 **Processor** means an entity which Processes Personal Data on behalf of the Controller;

1.12 **Restricted Transfer** means a transfer of Personal Data from SolarWinds to Vendor where such transfer would be prohibited by Data Protection Laws in the absence of the protection for the transferred Personal Data afforded pursuant to this DPA;

1.13 **SCC** means, as the context requires or otherwise indicated in this DPA, (i) Module 2 of the EU standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, attached in **Exhibit 1** hereto, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws ("**Module 2 SCC**").

1.14 **Services** means any Vendor product, service offering, or support service provided to SolarWinds as described in the Agreement;

1.15 **State Privacy Laws** means means US state privacy laws, which may include but shall not be limited to, the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., as amended including by the California Privacy Rights Act (the "**CCPA**"), the Virginia Consumer Data Protection Act, Code of Virginia title 59.1, Chapter 52 (the "**VCDPA**"), the Colorado Privacy Act, Colorado Rev. Stat. 6-1-1301 et seq. (the "**CPA**"), the Utah Consumer Privacy Act, Utah Code 13-61-101 et seq. ("**UCPA**"), the Connecticut Act Concerning Personal Data Protection and Online Monitoring, Conn. PA 22-15 § 1 et seq. ("**PDPOM**"), or any regulations or guidance issued pursuant thereto;

1.16 **Subprocessor** means any Processor (including any Vendor Affiliate) that Vendor engages to Process Personal Data in connection with the Services, and includes a "subcontractor" as that term is used in CCPA;

1.17 **Swiss Addendum** means the terms set out at Exhibit 3.

1.18 **Swiss Data Protection Law** means CH-DPA including its implementing ordinance and other data protection or privacy legislation in force in the Swiss Confederation, as may be amended from time to time;

1.19 **Restricted Swiss Data Transfer** means a transfer of Personal Data which falls within the scope of Swiss Data Protection Law to a third country which does not ensure an adequate level of data protection from a Swiss law perspective.

1.20 **Supervisory Authority** means (a) an independent public authority which is established by a member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws in the UK or Switzerland; (c) or any other relevant data authority;

1.21 **UK** means the United Kingdom of Great Britain and Northern Ireland; and

1.22 **UK Addendum to the SCCs** means the international data transfer addendum to the European Commission's standard contractual clauses for the transfer of personal data to third countries, as approved by the UK Parliament and published by the UK Information Commissioner's Office ("**ICO**"), attached in Exhibit 2 hereto, as amended or revised from time to time by the ICO.

1.23 The terms "business," "business purpose," "commercial purpose," "sell," "service provider," and "share" shall have the meanings given to those terms in the State Privacy Laws to the extent such meanings are materially similar to terms' meanings in CCPA, VCDPA, CPA, UCPA, or PDPOM. In the event of a conflict in the meanings of terms in the State Privacy Laws, the parties agree that the definition in the applicable State Privacy Law shall apply to the extent of the conflict.

## 2. Processing.

**2.1 Roles of the Parties.** The parties agree, regarding the Processing of Personal Data under relevant Data Protection Laws and this DPA, that (i) SolarWinds determines the purposes and means of Processing and is the Controller and (ii) Vendor is a Processor or service provider Processing Personal Data on SolarWinds's behalf. Vendor will comply with its applicable obligations under Data Protection Laws. Vendor shall process Personal Data only on SolarWinds's documented instructions, including with regard to transfers to a third country or international organization, unless otherwise required by applicable law, in which case Vendor will inform SolarWinds of that requirement unless prohibited on important grounds of public interest. For the avoidance of doubt the Agreement between SolarWinds and Vendor, and of which this DPA forms a part, constitutes documented instructions on which Vendor may process Personal Data. Vendor will immediately inform SolarWinds if Vendor has reason to consider that an instruction infringes Data Protection Laws.

**2.2 Sub-processing.** Vendor may engage Sub-processors pursuant to Section 5 below.

**2.3 Processing Details.** The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are described in Exhibit 1, Annex I to this DPA.

**3. Data Subject Rights.** Vendor will promptly notify SolarWinds if it receives a Data Subject Request and provide reasonable efforts to assist SolarWinds in responding to such Data Subject Request. Vendor is responsible for any costs arising from its provision of assistance to SolarWinds.

**4. Personnel.** Vendor will (i) restrict its personnel from Processing Personal Data without authorization (unless required by applicable law) and (ii) ensure personnel engaged to Process Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and are subject to appropriate contractual confidentiality obligations.

## 5. Sub-Processors.

**5.1 Appointment of Sub-processors.** SolarWinds (i) authorizes Vendor's Affiliates to be retained as Sub-processors, and (ii) authorizes Vendor to engage Sub-processors in connection with Processing Personal Data, subject to the terms of this DPA; provided that Vendor has entered into a written agreement with the applicable Sub-processor containing obligations substantially similar to those in this DPA. Vendor shall be fully liable to SolarWinds for the performance of such Sub-processors' failure to fulfil their respective obligations.

**5.2 Current Sub-processors and Notification of New Sub-processors.** Vendor may use Sub-processors for its Services. Vendor will neither appoint nor disclose any Personal Data to a proposed Sub-processor except with SolarWinds' prior written consent; [SolarWinds hereby consents to the Sub-processors listed in [Vendor to provide list.]]. Vendor shall, upon request, provide SolarWinds such copies of the Vendors' agreements with Sub-processors (which may be redacted to remove confidential commercial information not relevant to this Addendum's requirements). Vendor shall notify SolarWinds in writing at least 30 (thirty) calendar days before any new or replacement Sub-processor is engaged to process Personal Data.

**5.3 Objection Right for New Sub-processors.** SolarWinds may object, in good faith, to Vendor's proposed use of a new or replacement Sub-processor by written notification to Vendor within

thirty (30) calendar days after receiving the notice set out in Section 5.2. If SolarWinds objects to a new Sub-processor, Vendor will use reasonable efforts to change SolarWinds's configuration or use of the Services to avoid Processing of Personal Data by the Sub-processor in question without restricting the Services in any way. If Vendor is unable to make a requested change within a reasonable period of time or if the Services are restricted as a consequence of the objection, SolarWinds may terminate the applicable order form(s) and/ or Agreement without penalty.

## **6. Security.**

**6.1 Vendor Obligations.** Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, Vendor shall maintain appropriate technical and organizational measures to protect the security, confidentiality and integrity of Personal Data, as described in Annex II hereto. Vendor regularly monitors compliance with these safeguards and will not materially decrease the overall security of the Services during the Term or make any substantive changes without SolarWinds's approval.

**6.2 Audit and Cooperation.** Upon SolarWinds's written request, Vendor shall demonstrate compliance with this DPA and shall permit and contribute to audits or inspections of Vendor's Processing of Personal Data under this DPA, provided, however: that (a) SolarWinds gives Vendor at least one week's written notice; (b) any audit or inspection will be conducted during normal business hours and shall not materially interfere with Vendor's operations; and (c) SolarWinds shall not be entitled access to any information that is subject to a confidentiality obligation under law. Vendor will cooperate and assist SolarWinds in fulfilling SolarWinds's obligations under applicable law to carry out a data protection impact assessment and/or consult the relevant supervisory authority regarding such assessment related to SolarWinds's use of the Services.

## **7. Data Security Incident and Notification.**

**7.1** If Vendor becomes aware of a Data Security Incident involving Personal Data, it shall (i) notify SolarWinds of the Data Security Incident in writing without undue delay but no later than thirty six (36) hours upon Vendor or any Sub-processor becoming aware of a Data Security Incident; and (ii) where possible, will use reasonable efforts to assist SolarWinds in complying with SolarWinds's obligations under Data Protection Laws, including mitigating the Data Security Incident's adverse effects. Vendor shall have a documented incident response program and provide SolarWinds with sufficient information to allow SolarWinds to meet any reporting or notification obligations or inform Data Subjects of the Data Security Incident. Vendor shall fully cooperate with SolarWinds and comply with all applicable Data Protection Laws at Vendor's expense to stop or mitigate the effect of the Data Security Incident.

**7.2** Vendor will co-operate with SolarWinds, to the extent reasonably requested and/or if required by Data Protection Laws, in notifying any Supervisory Authorities or Data Subjects following a Personal Data Breach. Vendor must maintain cyber-liability or breach insurance at the minimum levels specified in the Agreement. Vendor must further pay the costs (i) for notifying any Supervisory Authority or regulatory agency, (ii) for notifying any affected data subjects and, (iii) associated with mitigating the effects of the Data Security Incident.

## **8. Transfer Mechanisms.**

**8.1** SolarWinds (as "data exporter") and Vendor (as "data importer"), with effect from the commencement of the relevant transfer, hereby enter into (i) the Module 2 SCC in respect of any

Restricted Transfer from or on behalf of SolarWinds to Vendor governed by GDPR, and/or (ii) the UK Addendum to the SCCs in respect of any Restricted Transfer from or on behalf of SolarWinds to Vendor governed by UK Data Protection Law and/or (iii) the Swiss Addendum insofar as a Restricted Swiss Data Transfer is undertaken by the parties.. SolarWinds authorizes Restricted Transfers that are subject to the Module 2 SCC or the UK Addendum to the SCCs or the Swiss Addendum (as appropriate).

8.2 If, at any time, a Supervisory Authority or a court with competent jurisdiction over a party mandates that transfers of Personal Data from controllers in the EEA, Switzerland or UK to processors established outside the EEA, Switzerland or UK must be subject to specific additional safeguards (including but not limited to specific technical and organizational measures), the parties shall work together in good faith to implement such safeguards and ensure that any transfer of Personal Data is conducted with the benefit of such additional safeguards.

## 9. Termination Right.

9.1 This DPA remains in effect for the duration of the Agreement between the parties and so long as Vendor processes Personal Data. SolarWinds may terminate the SCC at SolarWinds's discretion by providing written notice to Vendor.

9.2 Vendor shall, at SolarWinds's choice, delete or return all SolarWinds's Personal Data to it after the termination of the Agreement or in any event after the end of the provision of processing services, and certify that this has been done, unless Vendor is required by law to store copies of the Personal Data.

## 10. CCPA Provisions

10.1 This Section 10 (CCPA Provisions) supplements this DPA with additional provisions applicable to any Processing governed by the CCPA. In the event of any conflict between this Section and the remainder of this DPA, the provisions of this Section shall govern.

10.2 **Roles.** The parties agree that Vendor is a service provider and SolarWinds is a business.

10.3 **Vendor Responsibilities.** Vendor agrees that:

10.3.1 it shall not sell or share Personal Data;

10.3.2 it shall not collect, retain, use, disclose or otherwise Process Personal Data: (i) for any purpose (including a commercial purpose) other than for the specific purpose of performing the Services and obligations for the benefit of SolarWinds as specified in the Agreement, this DPA, or Exhibit 4 or (ii) outside of the direct business relationship between Vendor and SolarWinds;

10.3.3 it shall not combine Personal Data received from SolarWinds with Personal Data that Vendor receives from, or on behalf of, another person or persons, or collects from its own interactions with consumers, if any;

10.3.4 notwithstanding anything to the contrary in Section 3 (Data Subject Rights), it shall promptly refer to SolarWinds any requests received from consumers with respect to Personal Data, including requests to access, delete, or change Personal Data. Upon notice from SolarWinds of a consumer request, which SolarWinds shall provide when required by the CCPA, Vendor agrees to (a)

reasonably cooperate with and reasonably assist SolarWinds in responding to and fulfilling such request, or (b) directly comply with the request;

- 10.3.5 SolarWinds shall have the right to take reasonable and appropriate steps to ensure that Vendor uses Personal Data in a manner consistent with SolarWinds' obligations under the CCPA, including by monitoring Vendor's compliance with this DPA through measures that may include manual reviews, automated scans, regular assessments, audits, or technical or operational testing (collectively for the purposes of this Section 10, "audit"). Vendor shall cooperate fully with any audit initiated by SolarWinds, provided that such audit will not unreasonably interfere with the normal conduct of Vendor's business;
- 10.3.6 Vendor agrees to notify SolarWinds no later than five (5) business days after Vendor determines that it can no longer meet its obligations under the CCPA. Upon receiving notice from Vendor in accordance with this subsection, SolarWinds may direct Vendor to take steps as reasonable and appropriate to remediate unauthorized Processing of Personal Data or terminate the Agreement upon thirty (30) days' notice; and
- 10.3.7 Vendor agrees to comply with all applicable sections of the CCPA, including providing the same level of privacy protection as required of SolarWinds under the CCPA.

## **11. Miscellaneous.**

The Agreement and this DPA apply only between the parties. Neither confer any rights to any other person or entity. This DPA does not modify the risk allocation agreed upon by the parties in the Agreement. The provisions of this DPA are supplemental to the Agreement. In the event of inconsistencies (i) between the provisions of the Agreement and the provisions of this DPA, the latter shall prevail; and (ii) between the provisions of this DPA and the provisions of the SCC, the latter shall prevail.

**[SIGNATURE PAGE FOLLOWS]**

On behalf of the data importer: **[Insert company name]**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organization)

On behalf of the data exporter: **SolarWinds Worldwide, LLC**

Name (written out in full):

Position: Director

Address: 7171 Southwest Parkway Building 400 Austin, Texas 78735

Other information necessary in order for the contract to be binding (if any): None

Signature: .....  
  
.....1E8FD9662115469.....

(stamp of organization)



**EXHIBIT 1****STANDARD CONTRACTUAL CLAUSES****SECTION I***Clause 1***Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>1</sup> for the transfer of personal data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

---

<sup>1</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

## *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 I.B.

### *Clause 7* **Docking clause**

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

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

### *Clause 8* **Data protection safeguards**

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

#### **8.1 Instructions**

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

#### **8.2 Purpose limitation**

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

### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### **8.4 Accuracy**

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

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

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

### **8.6 Security of processing**

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

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

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

## **8.7 Sensitive data**

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

## **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>2</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:

---

<sup>2</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.

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

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

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

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

#### *Clause 9*

##### **Use of sub-processors**

- (a) **OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.<sup>3</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.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### *Clause 10*

#### **Data subject rights**

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### *Clause 11*

#### **Redress**

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

---

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

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## *Clause 12*

### **Liability**

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



(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

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

### *Clause 13* **Supervision**

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(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<sup>4</sup>;
  - (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.

---

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

*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 securely 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**

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

*Clause 18*  
**Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX to EXHIBIT 1**EXPLANATORY NOTE:**

*It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.*

**ANNEX I****A. LIST OF PARTIES**

**Data exporter(s):** SolarWinds provides information, including Personal Data, to be processed by Data importer as part of the Services.

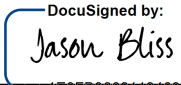
**Name:** SolarWinds Worldwide, LLC

**Address:** 7171 Southwest Parkway Building 400, Austin, Texas, 78735

**Tel.:** 1.866.530.8100

**E-mail:** privacy@solarwinds.com

**Activities relevant to the data transferred under these Clauses:** SolarWinds may provide information, including personal data, to be processed as part of the Services.

**Signature and date:**   
1E6FB9002113409...  
Role (controller/processor): Controller

**Data importer(s):** [Vendor to complete]

**Name:** [Vendor to complete]

**Address:** [Vendor to complete]

**Tel.:** [Vendor to complete]

**E-mail:** [Vendor to complete]

**Activities relevant to the data transferred under these Clauses:** [Vendor to complete]

**Signature and date:** \_\_\_\_\_  
Role (controller/processor): Processor

## B. DESCRIPTION OF TRANSFER

### Your obligations and rights

Your obligations and rights are set out in the Agreement and in this DPA.

### Subject matter and duration of the Processing of Personal Data

The subject matter of the processing is the performance of the Services pursuant to the Agreement. The duration of the processing is for the duration specified in the Agreement and in this DPA except where otherwise required by Data Protection Law.

### The nature and purpose of the Transfer and Processing of Personal Data; Processing operations

Data importer will process Personal Data in connection with providing the Services or fulfilling contractual obligations to SolarWinds pursuant to the Agreement and this DPA. The Personal Data transferred may be subject to the following basic processing activities, as may be further set forth in the Agreement: [Vendor to complete]

### Categories of data subjects whose personal data is transferred / processed

[Vendor to complete]

### Categories of personal data transferred; Types of Personal Data to be Processed

[Vendor to complete]

*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.*

[Vendor to complete]

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

[Vendor to complete]

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

[Vendor to complete]

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

[Vendor to complete]

## C. COMPETENT SUPERVISORY AUTHORITY

*Identify the competent supervisory authority/ies in accordance with Clause 13 of the Module 2 SCC*  
Supervisory Authority of the Member State where SolarWinds is established, or as otherwise determined in accordance with Clause 13, being the Data Protection Commissioner of Ireland.

## ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES

*Description of the technical and organisational measures implemented by the Contracted Processors (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

Data importer will maintain administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data as described in the hyperlink below. Data importer will not materially decrease the overall security of the Services during the subscription term.

<https://www.solarwinds.com/security/vendor-data-protection-requirements>



## EXHIBIT 2

### UK Addendum to the SCCs

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>       | The date of the Agreement.   |  |
| <b>The Parties</b>      | <b>Exporter (who sends the Restricted Transfer)</b>  | <b>Importer (who receives the Restricted Transfer)</b> |
| <b>Parties' details</b> | Please see page 7 of this DPA for the details of the Parties.  |  |
| <b>Key Contact</b>      | <p>The appropriate point of contact for the Exporter is set forth in in the signature block on page 7 of the DPA..</p> <p>The appropriate point of contact for the Importer is set forth in in the signature block on page 7 of the DPA.</p> |  |

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

| Addendum EU SCCs |   | This Addendum is appended to the version of the Approved EU SCCs as set out in Exhibit 1 of this Agreement, detailed below, including the Appendix Information: |                    |  |                         |  |
|------------------|---|---|--------------------|--|-------------------------|--|
| 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                | Where appropriate/required for the transfer | Yes   | No                 | General Authorisation                                    | 30 days                 |  |

**Table 3: Appendix Information**

“Appendix Information” means the information as set out in the Annexes of Exhibit 1 to this Agreement.

|  |
|--|
| <b>Annex 1A: List of Parties: Please see Page 7 of this DPA / Annex I.A of Exhibit 1.</b>  |
| <b>Annex 1B: Description of Transfer: Please see the information as set out in Annex I.B. of Exhibit 1 to this DPA.</b>  |
| <b>Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Please see the information as set out in Annex II of Exhibit 1 to this DPA.</b> |

**Annex III: List of Sub processors (Modules 2 and 3 only): Please see full list of Sub-processors set out here / maintained on the following website: [Vendor to provide]**

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

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

## **Part 2: Mandatory Clauses**

### Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex IA 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 it legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum (including by executing this agreement). Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

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

| <b>Addendum</b>                | <b>This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.</b>   |
|--------------------------------|--|
| <b>Addendum EU SCCs</b>        | The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.  |
| <b>Appendix Information</b>    | As set out in Table 3.   |
| <b>Appropriate Safeguards</b>  | 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. |
| <b>Approved Addendum</b>       | 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.   |
| <b>Approved EU SCCs</b>        | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and as incorporated into this Agreement under Exhibit 1.   |
| <b>ICO</b>                     | The Information Commissioner of the United Kingdom   |
| <b>Restricted Transfer</b>     | A transfer which is covered by Chapter V of the UK GDPR.   |
| <b>UK</b>                      | The United Kingdom of Great Britain and Northern Ireland.  |
| <b>UK Data Protection Laws</b> | 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.                                      |
| <b>UK GDPR</b>                 | 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.

**Exhibit 3 – Standard Contractual Clauses for the Transfer of Personal Data From the Swiss Confederation To Third Countries (Controller To Processor Transfers)**

1. If Personal Data falls within the scope of Swiss Data Protection Law and is transferred to a third country that does not ensure an adequate level of data protection under Swiss Data Protection Law, the Standard Contractual Clauses at Exhibit 1 will apply. In order for these Standard Contractual Clauses to comply with Swiss law and thus be suitable for ensuring an adequate level of protection for data transfers from Switzerland to a third country in accordance with the Swiss Federal Act on Data Protection ("CH-DPA"), these Clauses shall be amended with the following prevailing provisions:

- (a) The Parties adopt the standard of the Regulation (EU) 2016/679 for all Restricted Swiss Data Transfers .
- (b) Competent supervisory authority (Clause 13):
  - (i) To the extent the transfer of personal data is governed by the CH-DPA, the Swiss Federal Data Protection and Information Commissioner shall act as the competent supervisory authority.
  - (ii) To the extent the transfer of personal data is governed by the Regulation (EU) 2016/679, the Irish Data Protection Commission shall act as the competent supervisory authority.
- (c) Governing law (Clause 17): These Clauses shall be governed by the laws of Ireland as determined in Clause 17 of the Standard Contractual Clauses at Exhibit 1.
- (d) Choice of forum and jurisdiction (Clause 18.a/b): Any dispute arising from these Clauses shall be resolved by the courts of Ireland as determined in Clause 18.b of the Standard Contractual Clauses at Exhibit 1.
- (e) Data subject jurisdiction (Clause 18.c): The term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of pursuing their rights at their place of habitual residence (Switzerland) in accordance with Clause 18.c of the Standard Contractual Clauses at Exhibit 1. Accordingly, data subjects with their place of habitual residence in Switzerland may also bring legal proceedings before the competent courts in Switzerland.
- (f) Scope of "personal data" (Clause 1.a/c): In addition to personal data pertaining to natural persons, these Clauses shall be applicable to and protect personal data pertaining to legal entities as well, if and to the extent such personal data pertaining to legal entities is within the scope of the CH-DPA.

## EXHIBIT 4

### Details of Processing Subject to CCPA

|                                  |  |
|----------------------------------|--|
| <b>Purpose of the processing</b> | <p>CPRA Mandatory Disclosure: The specific business purposes are (select):</p> <p><input type="checkbox"/> <b>Auditing:</b> Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.</p> <p><input type="checkbox"/> <b>Security &amp; Integrity:</b> Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.</p> <p><input type="checkbox"/> <b>Repair Functionality:</b> Debugging to identify and repair errors that impair existing intended functionality.</p> <p><input type="checkbox"/> <b>Short-term, transient use:</b> Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.</p> <p><b>Performing services on behalf of Client:</b> Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business. <span style="background-color: yellow;">The specific services are: [Insert].</span></p> <p><input type="checkbox"/> <b>Advertising &amp; Marketing:</b> Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.</p> <p><input type="checkbox"/> <b>Internal Research:</b> Undertaking internal research for technological development and demonstration.</p> <p><input type="checkbox"/> <b>Quality &amp; Safety:</b> Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.</p> |
|----------------------------------|--|