CUSTOMER DATA PROCESSING ADDENDUM

Last revised 27 September 2021

This Data Processing Addendum ("DPA") is between SolarWinds Worldwide, LLC ("SolarWinds"), and the customer ("You," "Your," or "Company").

This DPA forms part of the Software Services Agreement ("Agreement"), entered into between SolarWinds and You, and applies to the extent that (i) SolarWinds processes Personal Data on behalf of You in the course of providing the Services or Software; and (ii) the Agreement expressly incorporates this DPA by reference. Information about SolarWinds' processing of Personal Data as a controller is set forth in our privacy notice available here https://www.solarwinds.com/legal/privacy.

This DPA serves as the final and entire expression of the parties' agreement on the subject matter hereof.

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

For Customers wishing to replace their DPA signed prior to 27 September 2021 with this updated DPA including Module 2 SCC:

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the DPA main body, Exhibit 1 (including Appendix) and Exhibit 2.

2. SolarWinds has pre-signed this DPA. SolarWinds, as the data importer, has also pre-signed the Standard Contractual Clauses (SCC) in Exhibit 1 and Exhibit 2.

3. To complete this DPA, You must:

    a. Complete the information in the signature boxes and sign on page 7.

    b. Sign on page 21.

    c. Send the completed and signed DPA to SolarWinds by email, indicating the Customer's Name and Account (as set out on the applicable SolarWinds Order Form or invoice) to privacy@solarwinds.com.

This DPA will become legally binding once SolarWinds receives Your validly completed DPA at privacy@solarwinds.com

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   **CCPA** means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199, as may be amended, supplemented or replaced from time to time;

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

1.4   **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) CCPA; in each case, as may be amended, supplemented or replaced from time to time. For the avoidance of doubt, if SolarWinds's processing activities involving Personal Data are not within the scope of an applicable law as set forth in this definition, such law is not applicable for purposes of this Addendum.

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

1.6   **Data Subject** means the identified or identifiable person to whom Personal Data relates;

1.7   **Data Subject Request** means a request from a Data Subject to exercise any right under relevant Data Protection Laws;

1.8   **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");

1.9   **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;

1.10   **Personal Data** means any information relating to an identified or identifiable natural person processed by SolarWinds on Your behalf pursuant to the Agreement;

1.11   **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;

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

1.13   **Restricted Transfer** means a transfer of Personal Data from You to SolarWinds 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;

1.14   **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**"), and/or (ii) the standard contractual clauses (processors) set out in Decision 2010/87/EC, attached in **Exhibit 2** hereto, as amended or replaced from time to time, pursuant to Article 46 of the UK GDPR ("**UK SCC**");

1.15   **Security, Privacy, and Architecture Documentation** means the SolarWinds Security Statement, available online at https://www.solarwinds.com/security/security-statement;

1.16   **Services** means any SolarWinds product, service offering, or support service provided to You pursuant to the Agreement; and

1.17   **Subprocessor** means any SolarWinds Affiliate and any Processor that SolarWinds or its Affiliates engage to Processes Personal Data in connection with the Services.

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) You determine the purposes and means of Processing and are the Controller and (ii) SolarWinds is a Processor or service provider (as defined in the CCPA) Processing Your Personal Data on Your behalf. Each party will comply with its applicable obligations under Data Protection Laws. SolarWinds shall process Personal Data only on Your documented instructions, including with regard to transfers to a third country or international organization, unless otherwise required by applicable law, in which case SolarWinds will inform you of that requirement unless prohibited on important grounds of public interest. SolarWinds will immediately inform You if SolarWinds has reason to consider that an instruction infringes Data Protection Laws, provided however that SolarWinds does not have any obligation to You to verify the compliance of any instruction with Data Protection Laws.

2.2   **Sub-processing.** SolarWinds and its Affiliates 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; Legal Disclosure Requests.

3.1   **Data Subject Rights.** If legally permitted, SolarWinds will promptly notify You if it receives a Data Subject Request to exercise their right under Data Protection Law ("Data Subject Request"). If You have access to the relevant Personal Data, You must respond to the Data Subject Request. If You are unable to address a Data Subject Request, SolarWinds will provide commercially reasonable efforts to assist You in responding to such Data Subject Request if legally permitted to and/or required to under relevant Data Protection Laws, upon written request. You are responsible for any costs arising from SolarWinds' provision of such assistance if a request is manifestly unfounded or excessive.

4.   Personnel.

SolarWinds 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 confidentiality obligations.

5.   Sub-Processors.

5.1   **Appointment of Sub-processors.** You (i) authorize SolarWinds's Affiliates to be retained as Sub-processors, and (ii) authorize SolarWinds and SolarWinds's Affiliates respectively to engage third-party Sub-processors in connection with Processing Personal Data; provided that SolarWinds or a SolarWinds Affiliate has entered into a written agreement with the applicable Sub-processor containing data protection obligations substantially similar to those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. SolarWinds shall be fully liable to You for the performance of such Sub-proccessors' failure to fulfil their respective data protection obligations.

5.2   **Current Sub-processors and Notification of New Sub-processors.** SolarWinds uses Sub-processors for its Services. They and their geographic locations are listed on our website ("Sub-processor List"), including a subscription mechanism for Sub-processor List updates.

5.3   **Objection Right for New Sub-processors**. You may reasonably object, in good faith, to SolarWinds's proposed use of a new Sub-processor by written notififcation to SolarWinds within ten (10) business days after receiving an updated Sub-processor List. If You object to a new Sub-processor, SolarWinds will use reasonable efforts to change Your configuration or use of the Services to avoid Processing of Personal Data by the Sub-processor in question. If SolarWinds is unable to make a requested change within a reasonable period of time, either party may terminate the applicable Order Form(s) limited only to those Services which SolarWinds cannot provide without using the new Sub-processor to which You objected.

6.   Security.

6.1   **SolarWinds Obligations.** Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, SolarWinds shall maintain approrpriate technical and organizational measures to protect the security, confidentiality and integrity of Personal Data, pursuant to the Security, Privacy and Architecture Documentation, herein incorporated by reference. SolarWinds regularly monitors compliance with these safeguards and will not materially descrease the overall security of the Services during the Term. You shall be responsible for implementing the appropriate technical and organizational measures for Your Processing of Personal Data as well as using and configuring the Services to comply with Data Protection Laws.

6.2   **Audit and Cooperation.** Upon Your written request, SolarWinds shall demonstrate compliance with this DPA and shall permit and contribute to audits or inspections of SolarWinds's Processing of Personal Data under this DPA, provided, however: that (a) You give SolarWinds at least two weeks' written notice; (b) any audit or inspection will be conducted during normal business hours and shall not interfere with SolarWinds operations; and (c) You shall not be entitled access to any information that is not Personal Data or that is subject to a confidentiality obligation under law or contract, including without limitation any such obligation owed to another customer of SolarWinds. Notwithstanding the foregoing, You shall be entitled to exercise Your rights under this Section 6.2 more than once per year during the term of the DPA in the event of a Data Security Incident or if required by a supervisory authority. SolarWinds will also reasonably cooperate and assist you in fulfilling Your GDPR obligations to carry out a data protection impact assessment and/or consult the relevant supervisory authority regarding such assessment related to Your use of the Services, if SolarWinds has such information and You do not have access to the relevant information.

7.   Data Security Incident and Notification.

If SolarWinds becomes aware of a Data Security Incident involving Personal Data , it shall (i) notify You of the Data Security Incident as soon as reasonably practical and in any case without undue delay; and (ii) where possible, will use reasonable efforts to assist You in complying with Your obligations under Data Protection Laws, including mitigating the Data Security Incident's adverse effects.

8.   Transfer Mechanisms.

8.1   You (as "data exporter") and SolarWinds (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 You to SolarWinds governed by GDPR, and/or (ii) the UK SCC in respect of any Restricted Transfer from You to SolarWinds governed by UK Data Protection Law.

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 to processors established outside the EEA 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.

8.3   If at any time the UK government approves the Module 2 SCC for use under the UK GDPR, the provisions of Module 2 SCC shall apply in place of the UK SCC in respect of Restricted Transfers subject to UK Data Protection Law, subject to any modifications to Module 2 SCC required by UK law (and subject to the governing law of Module 2 SCC being English law and the relevant supervisory authority being the Information Commissioner's Office).

9.   Termination Right.

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

10.   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.

11.   CCPA Provisions

11.1   This Section 11 (CCPA Provisions) applies solely to Personal Data of California residents as defined in Section 1798.140(g) of the CCPA.

11.2   The parties agree that SolarWinds is a Service Provider and You are a Business for CCPA purposes. SolarWinds shall not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing the Services; (iii) retain, use, or disclose Personal Data for a commercial purpose other than providing the Services; or (iv) retain, use, or disclose Personal Data outside of the direct business relationship between You and SolarWinds. By executing this DPA or the Agreement (as applicable), SolarWinds certifies that it understands these restrictions and will comply with them.

[SIGNATURE PAGE FOLLOWS]

On behalf of the data exporter:
Name (written out in full):

Position:

Address:

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

Signature…………………………………….

(stamp of organization)

On behalf of the data importer: SolarWinds Worldwide, LLC

Name (written out in full): Jason Bliss

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

Jason Bliss

Signature: …………………………………….

(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)[1] 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.

---

[1]   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[2] (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:

---

[2]   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

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 30in 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.

(a)   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.[3] 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.

(b)   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.

(c)   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.

(d)   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.

---

[3]   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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)   The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

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

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

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

   (ii)   the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

   (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).

---

[4]   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.

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

Clause 15
Obligations of the data importer in case of access by public authorities

15.1   **Notification**

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

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

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

(b)   If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)   The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   **Review of legality and data minimisation**

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

(b)   The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

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

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

  (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  (ii)   the data importer is in substantial or persistent breach of these Clauses; or
  (iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17
Governing law

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 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): Company is data importer's customer and provides information, including Personal Data, to be processed as part of the Services.

Activities relevant to the data transferred under these Clauses: You are data importer's customer and provide information, including personal data, to be processed as part of the Services.

Signature and date: _____

Role (controller/processor): Controller

1. **Data importer(s):** SolarWinds provides integrated cloud-based IT service management solutions that process Personal Data upon the instruction of the data exporter, in accordance with the terms of the Agreement.

2. **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 provides integrated cloud-based IT service management solutions that process Personal Data upon the instruction of the data exporter, in accordance with the terms of the Agreement.

Signature and date: _____*Jason Bliss*_____

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 of this Agreement 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 SolarWinds Services or fulfilling contractual obligations to Customer pursuant to the Agreement. The personal data transferred may be subject to the following basic processing activities, as may be further set forth in the Agreement: (a) hosting Personal Data, making it available to Customer for modification and transmission, and deleting Personal Data and other Services delivered to Company, including Services offered by means of products that help Customer monitor and manage its network, applications, systems, and information technology infrastructure (b) customer support and service activities, such as processing orders, and providing technical support.

Categories of data subjects whose personal data is transferred / processed
Data exporter may submit personal data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects, which personal data must beobtained, retained, and transmitted in accordance with the policies of the data exporter and with all legal requirements to which the data exporter is subject:

- Data exporter's Users;
- Data exporter's employees;
- Data exporter's consultants;
- Data exporter's contractors;
- Data exporter's agents; and
- Third parties with whom data exporter conducts business.

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

Any personal data comprised in Personal Data data exporter provides data importer. Personal data may include, but is not limited to, the following categories:

- First and last name
- Contact information (company, email address, phone and physical address)
- Financial information
- Account information
- IP and MAC address
- Browser information

- Product information, including localization data, network device information, activity logs, connection data, system usage and network data, application information, email data, traffic data, and other electronic data submitted, stored, uploaded, sent, or received by data exporter or data subjects via the Services

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.

None anticipated.

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

Continuous

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

The processing takes place from the commencement of the Agreement until deletion of all Personal Data by SolarWinds in accordance with the DPA and/or Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
See https://www.solarwinds.com/legal/legal-documents for information relating to sub-processors.

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 Company is established, or as otherwise determined in accordance with Clause 13

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 uploaded through the Services subscribed to or purchased by the data exporter, as described in the Security, Privacy, and Architecture Documentation applicable to the Services, which may be reasonably made available by data importer. Data importer will not materially decrease the overall security of the Services during the subscription term.

EXHIBIT 2

Standard Contractual Clauses (processors)

For purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: ....

Address: ....

Tel.:..

Fax:..

E-mail: ....

Other information needed to identify the organisation: ……………………………………………………………………………

(the data **exporter**)

and

Name of the data importing organisation: SolarWinds Worldwide, LLC

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

Tel.:   1.866.530.8100

E-mail: privacy@solarwinds.com

Other information needed to identify the organisation: None

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b)   '*the data exporter'* means the controller who transfers the personal data;

(c)   *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)   '*the applicable data protection law***'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)   *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the Transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party Beneficiary Clause

1.   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.   The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.   The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4.   The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The data exporter agrees and warrants:

(a)   that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

(i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii)   any accidental or unauthorised access, and

(iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1.   The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2.   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3.   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and Jurisdiction

1.   The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

2.   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with Supervisory Authorities

1.   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the Contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the Termination of Personal Data Processing Services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.   The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

See Annex I to Exhibit 1

Data Exporter.

Data Importer.

Data Subjects.

Categories of Data.

Special Categories of Data (if appropriate).

Processing Operations.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Annex II to Exhibit 1

Data importer will maintain administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data uploaded through the Services subscribed to or purchased by the data exporter, as described in the Security, Privacy, and Architecture Documentation applicable to the Services, which may be reasonably made available by data importer. Data importer will not materially decrease the overall security of the Services during the subscription term.