GDPR CONTROLLER/PROCESSOR CONTRACT ADDENDUM (KASEYA AS PROCESSOR)

DEFINITIONS

"**Customer Personal Data**" means any personal data that is subject to the Regulation processed by Kaseya on behalf of the Customer under the End User License Agreement to which and Customer are parties (the "Agreement").

"**Data Protection Laws**" means all applicable data protection and privacy legislation in force from time to time in (i) the UK (including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) ("**DPA 2018"**)); and (ii) in the EU (if and to the extent applicable to a party to this addendum when processing Customer Personal Data) (including without limitation the Regulation), in each case as amended from time to time "**Personal Data**", "**Processor**", "**Data Subject**", and "**Controller**" are as defined in the Regulation.

"**Regulation**" means Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation) or regulations of the United Kingdom, the United States, and laws similar in nature in other jurisdictions.

"**Regulator**" means the data protection supervisory authority that has jurisdiction over the Controller's or the Processor's processing of Personal Data.

DATA PROTECTION

1.1 [Customer Name] ("Customer") shall be the Controller and **Kaseya** ("Service Provider") shall be the Processor regarding any Personal Data processed by Service Provider on Customer's behalf under the Agreement.

1.2 Customer represents and warrants that the processing to be undertaken pursuant to this Agreement is consistent with the principles for personal data processing set forth in Art. 5 of the Regulation, including that the Customer has a lawful basis for any processing activities it directs Service Provider to undertake, and has provided appropriate notification to data subjects.

1.3 In respect of Customer Personal Data, Service Provider shall: (i) act only on Customer's written instructions; (ii) not process Customer Personal Data for any purpose other than in connection with the provision of the applicable Software and Services and performance of the obligations under the Agreement; (iii) notify Customer promptly if: (a) it receives a legally binding request for disclosure of Customer Personal Data by a law enforcement authority unless otherwise prohibited; (b) it is of the opinion that an instruction from Customer violates applicable European Union or Member State law, unless it is legally prohibited from notifying Customer on important grounds of public interest.

1.4 Service Provider shall: (i) ensure that all Service Provider personnel who have access to Customer Personal Data are bound by the duty of confidentiality; (ii) ensure that Service Provider personnel do not process Customer Personal Data except on instructions from Customer, unless they are required to do so by European Union or Member State law; (iii) provide training to Service Provider personnel regarding this Addendum.

1.5 Service Provider shall: (i) not disclose Customer Personal Data to any of its personnel or any third party except as necessary to perform the Services, to comply with European Union or Member State law to which it is subject, or with Customer's prior written consent; (ii) implement and maintain technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, access or processing in accordance with Article 32 of the Regulation; (iii) provide reasonable assistance to Customer in implementing its own technical and organisational measures.

1.6 Service Provider shall without undue delay notify Customer in writing of any Personal Data Breach (as such term is defined in the Regulation). Service Provider will provide all reasonable assistance to Customer regarding any Personal Data Breach. Service Provider will also provide all reasonable assistance to Customer in relation to its obligations to notify Regulators and affected Data Subjects.

1.7 Service Provider shall have in place appropriate measures to assist Customer in complying with its obligations to respond to requests for exercising Data Subjects' rights under the Regulation. Service Provider shall notify Customer of any request made by a Data Subject to exercise any Data Subject right under the Regulation ("**Data Subject Request**") and shall cooperate with Customer to execute its obligations under the Regulation in relation to such Data Subject Requests.

1.8 Service Provider shall provide such co-operation as necessary to enable Customer to verify Service Provider's compliance with the Regulation. Such co-operation may include helping Customer to carry out audits of Service Provider's data processing operations, such as by permitting Customer or its authorised auditors or Regulators to inspect those operations.

1.9 Service Provider shall assist Customer in complying with any obligations under the Data Protection Laws, including obligations to investigate, remediate and provide information to Regulators or Data Subjects about Personal Data Breaches without undue delay, to carry out data privacy impact assessments and to consult with Regulators regarding processing which is the subject of a data privacy impact assessment.

1.10 No Customer Personal Data processed within the European Economic Area by Service Provider pursuant to this Agreement shall be exported outside the European Economic Area without the prior written permission of Customer. Where that permission is given, it shall be conditional on any export being carried out on the terms of the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by the European Commission's Decision (EU) 2021/914 of 4 June 2021, whose Appendices 1 and 2 are exhibited in this Agreement (the "Clauses"). The Clauses are hereby incorporated by reference and will be binding on the parties. In case of conflict between the Agreement and the Clauses, the Clauses shall prevail.

1.11 Customer hereby authorizes Service Provider to subcontract the processing of Customer Personal Data, so long as Service Provider: (i) ensures that it has a written contract (the "**Processing Contract**") in place with the relevant subprocessor which meets the requirements of Data Protection Laws and which imposes on the subprocessor the same obligations in respect of processing of Customer Personal Data as are imposed on Service Provider under this Agreement; and (ii) remains liable to Customer for acts or omissions of the subprocessor under the Processing Contract. From time to time, and for any reason, Service Provider may add or replace subprocessors ("Subprocessor Change"). Service Provider shall notify Customer of a Subprocessor Change ("Change Notice"). Customer shall have ten (10) days from receipt of the Change Notice to object, in writing to Service Provider, to the Subprocessor Change ("Customer Objection"). The Customer Objection must specifically describe Customer's objection(s) to the Subprocessor Change. If in Service Provider's discretion, Customer fails to provide specific reasons for its objections in its Customer Objection or Customer's stated objections are insufficient under then-existing law or regulation, then Service Provider shall be permitted to proceed with the Subprocessor Change. Customer acknowledges and agrees that if Service Provider is unable to proceed with a Subprocessor Change due to the Client's Objection, then Service Provider may, in its discretion, (i) modify its proposed Subprocessor Change to accommodate the Customer Objection and proceed with the Subprocessor Change as modified; (ii) terminate the applicable services agreement (and proceed under the applicable termination procedures in the services agreement); or (iii) unilaterally modify the fees under the applicable services agreement to accommodate the Customer Objection.

1.12 Service Provider shall delete or return Customer Personal Data to Customer after the end of the provision of the Services, save where it is required to retain such data for compliance with applicable European Union or Member State law.

Acknowledged and Agreed:

Kaseya	**[Customer Name]**
By: _____	**By:** _____
(Authorized Signature)	(Authorized Signature)
Name: _____	**Name:** _____
(Print or Type)	(Print or Type)
Title: _____	**Title:** _____

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

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 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f); (v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b);

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 – [RESERVED]

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 organizational measures, to satisfy its obligations under these Clauses.

Transfer controller to processor

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.

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 ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 **Documentation and compliance**

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

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

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

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

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

Clause 9

Use of sub-processors

Transfer controller to processor

(a) 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 fifteen (15) 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. ([8]) 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 11

Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

Transfer controller to processor

(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

Transfer controller to processor

(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 ([12]);

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

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

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

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

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

Clause 15

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

15.1 **Notification**

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

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

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

For Module Three: The data exporter shall forward the notification to the controller.

(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.). For Module Three: The data exporter shall forward the information to the controller.

(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. For Module Three: The data exporter shall make the assessment available to the controller.

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow 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

ANNEX I

A. **LIST OF PARTIES**

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

1. Name: **[Customer Name]**
Address: Contact person's name, position and contact details: .....
.....

Activities relevant to the data transferred under these Clauses: Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Kaseya Software and Services under the Kaseya Master Services Agreement.

Signature and date: .....

Role (controller/processor): Controller

2. .....

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

1. Name: Kaseya

Address: 701 Brickell Ave #400, Miami, FL 33131

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Kaseya Software and Services under the Kaseya Master Services Agreement.

Signature and date: .....

Role (controller/processor): Processor

2. .....

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

[to be provided by the controller]

Categories of personal data transferred

[to be provided by the controller]

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.

[to be provided by the controller]

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

Data transfer is continuous for Kaseya products.

Nature of the processing

Data importer processes data in accordance with the Agreement at the direction of data exporter to provide IT services and software.

Purpose(s) of the data transfer and further processing

Data importer processes categories of personal data are in accordance with the Agreement at the direction of data exporter.

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

Data shall be retained by the processor for the life of the agreement plus 30 days.

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

Data importer utilizes sub processors for hosting and colocation services.

C. **COMPETENT SUPERVISORY AUTHORITY**

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

The supervisory authority is the Irish Data Protection Commission.

ANNEX I

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

Kaseya maintains an information security, privacy, and compliance program aligned with Kaseya's business objectives and in accordance with ISO/IEC 27000 standards and NIST Cybersecurity Framework. Kaseya's technical and organizational measures are regularly tested and evaluated by independent third-party auditors, including penetration tests and annual AICPA SOC 2 Type II audits. Measures are also regularly tested by internal audits, as well as annual and targeted risk assessments.

Kaseya's information security program includes:

Measures of encryption of Personal Data

Kaseya designs, implements, and effectively operates encryption to adequately protect Personal Data in transit or at rest by:

- Using state-of-the-art encryption protocols and algorithms designed to provide effective protection against active and passive attacks with resources known to be available to public authorities.
- Using trustworthy public-key certification authorities and infrastructure.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Kaseya enhances the security of processing systems and services in production environments by:

- Employing a code review process before promoting code to product to increase the security of the code used to provide the Services.
- Testing code and systems for vulnerabilities before and during use.
- Maintaining an external Vulnerability Disclosure Policy.
- Using checks to validate the integrity of encrypted data.
- Employing preventative and reactive intrusion prevention and detection systems.
- Deploying high-availability systems across geographically distributed data centers.

Kaseya designs, implements, and effectively operates access control measures to protect and maintain the confidentiality of Personal Data by:

- Adopting the least privilege access principle on a need-to-know basis.
- Implementing an access control and policy for the creation, reading, updating, and deletion of data.
- Authenticating authorized and identified personnel using unique authentication credentials (passwords) and two factor authentication whenever possible.
- Automatically signing-out user IDs after a period of inactivity.
- Maintaining data processing facilities – data centers, server rooms, and telecommunication rooms - locked and secure.
- Maintaining policies and training in respect of each employee's access rights to the Personal Data.
- Monitoring access and actions of those authorized to add, modify, or delete Personal Data.
- Controlling access to data, with controlled and documented destruction of data.

Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

Kaseya designs, implements, and effectively operates measures to ensure that Personal Data is protected from accidental destruction or loss by maintaining:

- Maintaining and testing business continuity plans / disaster recovery plans and procedures.
- Maintaining and testing incident management plans and procedures.
- Utilizing geographically distributed data centers.
- Using redundant infrastructure, including power supplies and internet connectivity.
- Storing backups at alternative sites and available for restore in case of failure of primary systems.

Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Kaseya's technical and organizational measures are regularly tested and evaluated by independent third-party auditors, including penetration tests and annual AICPA SOC 2 Type II audits. Measures are also regularly tested by internal audits, as well as annual and targeted risk assessments.

Measures for user identification and authorization

Kaseya designs, implements, and effectively operates measures for user authentication and privilege management by:

- Applying a mandatory access control and authentication policy.
- Authenticating authorized personnel using unique authentication credentials and strong two-factor authentication.
- Allocating and managing appropriate privileges according to role, approvals, and exception management.
- Applying the Adopting the least privilege access principle on a need-to-know basis.

Measures for the protection of data during transmission

Kaseya designs, implements, and effectively operates measures to protect Personal Data from being read, copied, modified, or deleted by unauthorized parties during transmission, including by:

- Using state-of-the-art transport encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities.
- Using trustworthy public-key certification authorities and infrastructure.
- Implementing protective measures against active and passive attacks on the sending and receiving systems providing transport encryption, such as layer 7 firewalls, IPS/IDS, threat management and traffic monitoring tools, anti-virus, anti-phishing and email security, mutual TLS encryption, API authentication, and encryption to protect the gateways and pipelines through which data travels, as well as testing for software vulnerabilities and possible backdoors.
- Using correctly implemented and properly maintained software, covered under a vulnerability management program.
- Enforcing secure measures to reliably generate, manage, store, and protect encryption keys.
- Audit logging, monitoring, and tracking data transmissions.

Measures for the protection of data during storage

Kaseya designs, implements, and effectively operates measures to protect Personal Data during storage, controlling and limiting access to data processing systems, and by:

- Using state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities.
- Using trustworthy public-key certification authorities and infrastructure.
- Testing systems storing data for software vulnerabilities and penetration.
- Using correctly implemented and properly maintained software, covered under a vulnerability management program.
- Enforcing secure measures to reliably generate, manage, store, and protect encryption keys.
- Identifying and authorizing systems and users with access to data processing systems.
- Automatically signing-out users after a period of inactivity.
- Audit logging, monitoring, and tracking access to data processing and storage systems.

Measures for ensuring physical security of locations at which Personal Data are processed

Kaseya designs, implements, and effectively operates physical access control policies and measures to prevent unauthorized persons from gaining access to the data processing equipment where the Personal Data are processed or stored, including by partnering with data center and cloud service providers that:

- Are renowned for excellency of services and physical security controls.
- Maintain state-of-the-art data centers with advanced physical access controls, including physical barriers, video surveillance systems, electronic intrusion detection systems.
- Provide redundancy and replication of data within or across regions.
- Maintain and monitor operational support systems, such as redundant electrical power systems, temperature humidity monitoring and control, fire detection and suppression systems, and leakage detection.
- Are independently tested by third-party organizations, possessing SOC 2 Type 2 reports or ISO/IEC 27001 certifications.
- Are compliant with privacy regulations, including CCPA and GDPR.

Measures for ensuring events logging

Kaseya designs, implements, and effectively operates a logging and monitoring program to log, monitor and track access to personal data, including by system administrators, and to ensure data is processed in accordance with instructions received. This is accomplished by various measures, including:

- Authenticating authorized and identified personnel using unique authentication credentials (passwords) and two factor authentication whenever possible.
- Maintaining updated lists of system administrators' identification details.
- Adopting measures to detect, assess, and respond to high-risk anomalies.
- Keeping secure, accurate, and unmodified access logs to the processing infrastructure.
- Testing the logging configuration, monitoring system, alerting and incident response process at least once annually.

Measures for ensuring system configuration, including default configuration

Kaseya designs, implements, and effectively operates configuration baselines for all systems supporting the production data processing environment, including third-party systems. Configuration baselines should align with industry best practices such as the Center for Internet Security (CIS) Level 1 benchmarks. Automated mechanisms must be used to enforce baseline configurations on production systems, and to prevent unauthorized changes. Changes to baselines are limited to a small number of authorized Kaseya personnel and must follow change control processes. Changes must be auditable and checked regularly to detect deviations from baseline configurations.

Kaseya configures baselines for the information system using the principle of least privilege. By default, access configurations are set to "deny-all," and default passwords must be changed to meet Kaseya's policies prior to device installation on the Kaseya network, or immediately after software or operating system installation. Systems are configured to synchronize system time clocks based on International Atomic Time or Coordinated Universal Time (UTC), and access to modify time data is restricted to authorized personnel.

Measures for internal IT and IT security governance and management

Kaseya maintains internal policies on the acceptable use of IT systems and general information security. Kaseya requires all employees and contractors to undertake general security and privacy awareness training at least every year, security awareness campaigns on a quarterly-basis, and make available monthly security awareness newsletters. Kaseya restricts and protects the processing of Personal Data, and has documented and implemented:

- Information security, privacy, and compliance programs in order to protect the confidentiality, integrity, and availability of Kaseya's data and information systems, and to ensure the effectiveness of security controls over data and information systems that support operations, both as a processor and a controller of customer information.

Kaseya keeps documentation of technical and organizational measures in case of audits and for the conservation of evidence. Kaseya shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Annex 2.

Measures for certification/assurance of processes and products

The implementation of Kaseya's information security, privacy, and compliance programs and related security risk management processes have been externally certified by annual AICPA SOC 2 Type II audits in accordance with the AICPA Trust Service Criteria, and details of these and other certifications that Kaseya may undertake from time to time will be made available on Kaseya's Trust center website.

Measures for allowing data portability and ensuring erasure

Kaseya designs, implements, and effective operates measures to allow data portability and ensuring erasure when technically possible and contractually agreed upon by:

- Restoring or exporting data stored in Kaseya's servers to customers' servers.
- Utilizing a NIST 800-88 based data destruction process in up to 30 days after the end of the agreement.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

Name	**Location(s)**	**Description of Processing**
Access Alto, provided by CoreSite Realty Corporation (d.b.a. Telehouse)	UK, US (New Jersey)	Hosting services
Access Alto, provided by Equinix, Inc.	Canada, Ireland, UK	Hosting and Colocation services
Aligned Energy	US (Utah)	Hosting and Colocation services
Allied Energy	UT US	Hosting
Amazon Web Services	US (East & West), Ireland, Australia, Canada	Hosting
Atlassian	US	Ticketing
CloudAMQP	US, UK, Australia, Canada, Singapore, Germany	SaaS Services
Coresite	US (San Jose, CA)	Hosting and Colocation services
Cyxtera	Slough UK	Hosting and Colocation services
DSM Technology Consultants	US (Florida)	Hosting and Colocation services
EdgeConneX	Munich, DE	Hosting and Colocation services
Equinix	Calgary, CA, Sydney, AU, Slough, UK, Singapore, US (Ashburn, VA)	Hosting and Colocation services
eStructure	Toronto CA	Hosting
eStruxture	Toronto, CA	Hosting and Colocation services
Faction Inc.	US (Colorado, Virginia),	Hosting and Collocation services
Faction Inc., provided by Equinix, Inc.	Germany	Hosting and Collocation services
IBM Enterprise and Technology Security	Australia, Germany, UK	Hosting and Colocation services
Kaseya	US	Support & Operations
Microsoft Azure	US, US (US West), UK, Australia, Canada, Singapore, Germany	Hosting and Colocation services
Monday.com	US	Internal Ticketing
NetSuite	US (NA West)	Billing and Financial reporting
NextDC	Melbourne, AU	Hosting and Colocation services
Nianet/GlobalConnect	Glostrup, DK, Glostrup, DK,	Hosting and Colocation services

Noris Network	Munich, DE	Collocation services
Noris Network, AG	Germany	Hosting
OneTrust	US (Azure)	Data Privacy Request System
Salesforce	US (Phoenix, USA / Washington DC, USA)	Sales CRM
Salesforce-Heroku	US (AWS US East), Ireland (AWS EU-Ireland)	SaaS Providor
Snowflake	US (AWS US East), Ireland (AWS EU-Ireland)	SaaS Providor
Sungard	US (Philadelphia, PA), Woking, UK	Hosting and Colocation services
SunGard Availability Services	PA US, Woking UK	Hosting
Tierpoint	US(New York, NY, Pennsylvania,)	Hosting and Colocation services
Verne Global	Reykjavík, IS	Hosting and Colocation services
Zayo Group LLC	US (Colorado, Georgia)	Collocation services
Zendesk	US (AWS)	Customer ticketing

Information Commissioner's Office

1. STANDARD DATA PROTECTION CLAUSES TO BE ISSUED BY THE COMMISSIONER UNDER S119A(1) DATA PROTECTION ACT 2018

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

VERSION B1.0, in force 21 March 2022

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

1.2 Part 1: Tables

(a) Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: **[Customer Name]** Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Kaseya Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

(b) Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is

	appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

(c) **Table 3: Appendix Information**

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

Annex 1A: List of Parties:

Annex 1B: Description of Transfer:

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

(d) **Table 4: Ending this Addendum when the Approved Addendum Changes**

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☐ neither Party

1.3 **Part 2: Mandatory Clauses**

(a) **Entering into this Addendum**

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

(b) **Interpretation of this Addendum**

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

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

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

(c) **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.

(d) **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.

(e) **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.

1.4 **Alternative Part 2 Mandatory Clauses:**

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