DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") governs the Processing of Personal Data by Revalize, Inc. and its Affiliates ("Provider") for the organization agreeing to the terms of this DPA ("Customer"). Provider and Customer are each herein referred to individually as a "Party", or collectively as the "Parties".

Whereas the Parties have entered into an agreement for the provision of software and/or other services by Provider to Customer ("Agreement"), this DPA governs the rights and obligations of the Parties in relation to Processing of Personal Data undertaken in connection with the provision and receipt of such software and/or other services.

For and in consideration of the representations and promises of the parties set forth herein, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. DEFINITIONS.

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 Adequacy Decision means, for a jurisdiction with Privacy Laws that have data transfer restrictions, a decision that the Supervisory Authority or other body in such jurisdiction recognizes as providing an adequate level of data protection as required by such jurisdiction's Privacy Laws such that transfer to that country shall be permitted without additional requirements;

1.1.2 Affiliate means any entity which now or in the future controls, is controlled by, or is under common control with the signatory to this DPA, with "control" defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through the ownership of voting securities, by contract, or otherwise;

1.1.3 CCPA means the California Consumer Privacy Act of 2018 (California Privacy Act Cal Civ Code § 1798.100 et seq) and its implementing regulations;

1.1.4 Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data including "business" as that term is defined by the CCPA, and in the context of this DPA shall mean the Customer;

1.1.5 Data Processing Instructions means the Processing instructions set out in Annex I B;

1.1.6 Data Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller (including "service provider" as that term is defined by the CCPA), and in the context of this DPA shall mean Provider;

1.1.7 Data Subject means the identified or identifiable person to whom Personal Data relates (including "consumer" as that term is defined by the CCPA);

1.1.8 EU GDPR means all EU regulations applicable (in whole or in part) to the Processing of Personal Data such as Regulation (EU) 2016/679;

1.1.9 EU SCCs means the contractual clauses annexed to the European Commission's Implementing Decision 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 and set out as Appendix 1 to this DPA;

1.1.10 Information Security Schedule means the information security, technical and organizational measures specified in Annex II, as may be updated from time to time;

1.1.11 Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

1.1.12 Privacy Laws means all data protection and privacy laws and regulations applicable to the Personal Data in question, including (without limitation and as applicable) the EU GDPR, UK GDPR, and CCPA, in each case as amended, superseded or replaced from time to time.

1.1.13 Process or Processing means any operation or set of operations that is performed upon Personal Data in connection with the Services, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, as described in the Data Processing Instructions;

1.1.14 Restricted Transfer means:

1.1.14.1 a transfer of Personal Data from Customer or a Customer Affiliate to Provider; or

1.1.14.2 an onward transfer of Personal Data from Provider to a Sub processor, in each case, where such transfer would be prohibited by Privacy Laws in the absence of an

approved method of transfer (such as (a) an Adequacy Decision, (b) Standard Contractual Clauses, (c) by the terms of other recognized forms of data transfer agreements or processes under applicable Privacy Laws or (d) a permitted derogation), or would be in breach of the terms of such an approved method of transfer or permitted derogation;

1.1.15 Services means the services and other activities to be supplied to or carried out by or on behalf of Provider for Customer pursuant to the Agreement;

1.1.16 Standard Contractual Clauses means the contractual clauses approved by a Supervisory Authority pursuant to Privacy Laws, as may be updated from time to time, which permit the transfer of Personal Data where such transfer would otherwise be a Restricted Transfer;

1.1.17 Sub processor means any third party (including any third party and any Provider Affiliate) appointed by or on behalf of Provider to undertake Processing in connection with the Services, which are listed in Annex III;

1.1.18 Supervisory Authority means a public authority or government or quasi-governmental agency which is established in a jurisdiction under Privacy Laws with competence in matters pertaining to data protection;

1.1.19 Swiss Addendum means the addendum to the EU SCCs set out in Appendix 3 to this DPA.

11.1.20 UK Addendum means the UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the UK Data Protection Act 2018, a copy of which is set out in Appendix 2 to this DPA; and1.1.21 UK GDPR means the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018.

1.2 References to Annexes are to annexes of the EU SCCs.

2. PROCESSING OF PERSONAL DATA

2.1 Provider will not:

2.1.1 retain, use, disclose or otherwise Process Personal Data for any purpose (including its own commercial purposes) other than on Customer's documented instructions (as set out in this DPA and in the Agreement) unless Processing is required under applicable law and under the terms of the Standard Contractual Clauses (where applicable); or

2.1.2 sell Personal Data received from Customer or obtained in connection with the provision of the Services to Customer.

2.2 Customer on behalf of itself and each Customer Affiliate:

2.2.1 instructs Provider:

2.2.1.1 to Process Personal Data; and

2.2.1.2 in particular, transfer Personal Data to any country or territory; in each case as reasonably necessary for the provision of the Services and consistent with this DPA.

2.3 The Data Processing Instructions sets out the subject matter and other details regarding the Processing of the Personal Data contemplated as part of the Services, including Data Subjects, categories of Personal Data, special categories of Personal Data, Sub processors and description of Processing.

2.4 The parties acknowledge that Customer's transfer of Personal Data to Provider is not a "sale" of Personal Data within the meaning of applicable Privacy Laws (including the CCPA) and Provider provides no monetary or other valuable consideration to Customer in exchange for the Personal Data.

3. PROVIDER PERSONNEL

Provider shall ensure that persons authorized to undertake Processing of the Personal Data have:

3.1 Committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in respect of the Personal Data; and

3.2 Undertaken appropriate training in relation to protection of Personal Data.

4. SECURITY

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Provider shall in relation to the Personal Data implement appropriate technical and organizational measures designed to provide a level of security appropriate to that risk in the provision of the Services and for

the purposes of this DPA Provider's technical and organizational measures are set out in the Information Security Schedule.

4.2 In assessing the appropriate level of security, Provider shall take account in particular of the risks that are presented by Processing.

5. SUBPROCESSING.

5.1 Provider shall only appoint Sub processors which enable Provider to comply with Privacy Laws. Customer authorizes Provider to appoint Sub processors in accordance with this Section 5 subject to any restrictions or conditions expressly set out in the Agreement. Sub processors appointed as at the effective date of this DPA are listed in the Data Processing Instructions. Provider shall remain liable to Customer for the performance of Sub processors' obligations subject to the Agreement.

5.2 Notwithstanding any notice requirements in the Agreement, before Provider engages any new Sub processor, Provider shall give Customer notice of such appointment, including details of the Processing to be undertaken by the proposed Sub processor. Any new Sub processor shall be added to the following https://revalizesoftware.com/legal and notified to Customer via email. In addition to any other notifications, Provider may provide such notice by updating the list of Sub processors in the Data Processing Instructions. Customer may notify Provider of any objections (on reasonable grounds related to Privacy Laws) to the proposed Sub processor or Data Processing Instructions ("Objection"), within 15 days of the notification from Provider of the updated Sub processor list, then Provider and Customer shall negotiate in good faith to agree to further measures including contractual or operational adjustments relevant to the appointment of the proposed Sub processor or operation of the Services to address Customer's Objection. Where such further measures cannot be agreed between the parties within forty-five (45) days from Provider's receipt of the Objection (or such greater period agreed by Customer in writing), Customer may by written notice to Provider with immediate effect terminate that part of the Services which require the use of the proposed Sub processor or another part of the Services which are so terminated.

6. DATA SUBJECT RIGHTS.

6.1 Provider shall:

6.1.1 Upon becoming aware, promptly notify Customer if Provider receives a request from a Data Subject relating to an actionable Data Subject right under any Privacy Law in respect of Personal Data;

6.1.2 Not respond to that request except on the documented instructions of Customer or as required by a Supervisory Authority or under applicable law; and

6.1.3 Upon request from Customer where required by Privacy Laws and in the context of the Services, reasonably assist Customer in dealing with an actionable Data Subject rights request to the extent Customer cannot fulfil this request without Provider's assistance. Provider may fulfil this request by making available functionality (at Customer's expense) that enables Customer to address such Data Subject rights request without additional Processing by Provider. To the extent such functionality is not available, in order for Provider to provide such reasonable assistance, Customer must communicate such request in writing to Provider providing sufficient information to enable Provider (at Customer's expense) to pinpoint and subsequently amend, export or delete the applicable record.

7. PERSONAL DATA BREACH.

7.1 Provider shall notify Customer without undue delay upon Provider or any Sub processor confirming a Personal Data Breach, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Privacy Laws. Subject to Section 7.3 below, such notification shall as a minimum:

7.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

7.1.2 communicate the name and contact details of Provider's data protection officer or other relevant contact from whom more information may be obtained;

7.1.3 describe the likely consequences of the Personal Data Breach in so far as Provider is able to ascertain having regard to the nature of the Services and the Personal Data Breach; and

7.1.4 describe the measures taken or proposed to be taken to address the Personal Data Breach.

7.2 Provider shall co-operate with Customer and take such commercially reasonable steps as are necessary to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 Where and in so far as, it is not possible to provide the information or Provider is prohibited by law or law enforcement from providing the information referred to in Section 7.1 at the same time, the information may be provided in phases without undue further delay.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION.

8.1 To the extent necessary, Provider shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Privacy Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, Provider. To the extent that such impact assessment and/or prior consultation requires assistance beyond Provider providing the applicable Provider processing record(s) and Documentation, Provider shall reserve the right to charge Customer such engagement at Provider's then current daily rates.

9. DELETION OR RETURN OF PERSONAL DATA.

9.1 Within thirty (30) days from termination or expiry of the Agreement (the "Return Period"), and subject to Section 9.2 below, at Customer's request, Provider will either delete or return available Personal Data. At the expiry of the Return Period, if Customer has not elected either of the foregoing Provider may delete and destroy all Personal Data without notice or liability to Customer. Where Customer requests Provider return available Personal Data, Provider may fulfil this request by making available functionality that enables Customer to retrieve the Personal Data without additional Processing by Provider. If Customer declines to use this functionality, Customer may, within the Return Period, request that Provider return the available Personal Data under an Order for the applicable professional services. In the event the Agreement is terminated for Customer's breach, Provider shall have the right to require that Customer prepay for such professional services. Provider shall provide written confirmation to Customer that it has fully complied with this Section 9 within thirty (30) days of Customer's request for such confirmation.

9.2 Provider may retain Personal Data to the extent required by Privacy Laws or any other statutory requirement to which Provider is subject and only to the extent and for such period as required by Privacy Laws or any other statutory requirement to which Provider is subject and always provided that (a) during such retention period the provisions of this DPA will continue to apply, (b) that Provider shall ensure the confidentiality of all such Personal Data, and (c) Provider shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Privacy Laws requiring its storage or any other statutory requirement to which Provider is subject and for no other purpose.

10. REVIEW, AUDIT AND INSPECTION RIGHTS.

10.1 Upon Customer's reasonable request, Provider shall provide all relevant and necessary material, documentation and information in relation to Provider's technical and organizational security measures used to protect the Personal Data in relation to the Services provided in order to demonstrate compliance with Privacy Laws. Such information may be provided in summary form to minimize the risk of such measures being circumvented.

10.2 Provider shall ensure a security audit of its technical and organizational security measures is carried out at least annually in compliance with Privacy Laws. The results of such security audit will be documented in a summary report. Provider shall promptly provide Customer upon request with (i) a confidential summary of such report; and (ii) evidence of appropriate remediation of any critical issues within four (4) weeks from date of issuance of the audit report.

10.3 If, following the completion of the steps set out in Sections 10.1 and 10.2, Customer reasonably believes that Provider is non-compliant with Privacy Laws, Customer may request that Provider make available, either by webinar or in a face-to-face review, extracts of all relevant information necessary to further demonstrate compliance with Privacy Laws. Customer undertaking such review shall give Provider reasonable notice, by contacting Provider's Information Security Director at privacy@revalizesoftware.com, and any review will be conducted under this Section 10.3.

10.4 In the event that Customer reasonably believes that its findings following the steps set out in Section 10.3 do not enable Customer to comply materially with Customer's obligations mandated under the Privacy Laws in relation to its appointment of Provider, then Customer may give Provider not less than thirty (30) days prior written notice of its intention,

undertake an audit which may include inspections of Provider to be conducted by Customer or an auditor mandated by Customer (not being a competitor of Provider). Such audit and/or inspection shall (i) be subject to confidentiality obligations agreed between Customer (or its mandated auditor) and Provider, (ii) be undertaken solely to the extent mandated by, and may not be further restricted under applicable Privacy Laws, (iii) not require Provider to compromise the confidentiality of security aspects of its systems and/or data processing facilities (including that of its Sub processors), and (iv) not be undertaken where it would place Provider in breach of Provider's confidentiality obligations to other Provider customers vendors and/or partners generally or otherwise cause Provider to breach laws applicable to Provider. Customer (or auditor mandated by Customer) undertaking such audit or inspection shall avoid causing any damage, injury or disruption to Provider's premises, equipment, personnel and business in the course of such a review. To the extent that such audit performed in accordance with this Section 10.4 exceeds one (1) business day, Provider shall reserve the right to charge Customer for each additional day at its then current daily rates.

10.5 If following such an audit or inspection under Section 10.4, Customer, acting reasonably, determines that Provider is non-compliant with Privacy Laws then Customer will provide details thereof to Provider upon receipt of which Provider shall provide its response and to the extent required, a draft remediation plan for the mutual agreement of the parties (such agreement not to be unreasonably withheld or delayed; the mutually agreed plan being the "Remediation Plan"). Where the parties are unable to reach agreement on the Remediation Plan, or in the event of agreement, Provider materially fails to implement the Remediation Plan by the agreed dates which in either case is not cured within forty-five (45) days following Customer's notice or another period as mutually agreed between the Parties, Customer may terminate the Services in part or in whole which relates to the non-compliant Processing and the remaining Services shall otherwise continue unaffected by such termination.

10.6 The rights of Customer under this Section 10 shall only be exercised once per calendar year unless Customer reasonably believes Provider to be in material breach of its obligations under either this DPA or Privacy Laws.

11. RESTRICTED TRANSFERS.

11.1 Customer (as "data exporter") and Provider, as appropriate, (as "data importer") hereby agree that the applicable Standard Contractual Clauses shall apply in respect of any Restricted Transfer from Customer or any Customer Affiliate to Provider to the extent required by Privacy Laws. The parties agree that the provisions of the Standard Contractual Clauses shall apply to the Restricted Transfer. Where Personal Data is subject to the EU GDPR, the applicable Standard Contractual Clauses shall be the EU SCCs, and where Personal Data is subject to the UK GDPR, the applicable Standard Contractual Clauses shall be the UK Addendum, in each case completed as described herein and as set out in Annex I, Annex II and Annex III. Where Personal Data is subject to Swiss Federal Data Protection Act, the provisions of the Swiss Addendum shall apply.

11.2 For the purposes of Annex I or other relevant part of the applicable Standard Contractual Clauses, the Data Processing Instructions sets out the Data Subjects, categories of Personal Data, special categories of Personal Data, Sub processors and description of Processing (processing operations). Where the EU SCCs apply to transfers from the Customer or a Customer Affiliate to Provider, they will be completed as set out in Annex I. Optional clauses in the applicable Standard Contractual Clauses shall not apply unless otherwise set out in Annex I.

11.3 For the purposes of Annex II or other relevant part of the applicable Standard Contractual Clauses, the Information Security Schedule sets out the description of the technical and organizational security measures implemented by Provider (the data importer).

11.4 Wherever the applicable Standard Contractual Clauses enable a choice of law or jurisdiction, the laws and courts of Ireland shall apply, unless otherwise required under applicable Privacy Law.

11.5 Provider shall not make any Restricted Transfer of Personal Data that it has received under this DPA, unless it has lawful grounds to do so under applicable Privacy Laws. Such lawful grounds may include (a) an Adequacy Decision, (b) Standard Contractual Clauses, (c) the terms of other recognized forms of data transfer agreements or processes); or (d) any permitted derogation under Privacy Law.

12. OTHER PRIVACY LAWS.

12.1 To the extent that Processing relates to Personal Data originating from a jurisdiction or in a jurisdiction which has any mandatory requirements or introduces any such

requirements in the future, in addition to those in this DPA, both Parties may agree to any additional measures required to ensure compliance with applicable Privacy Laws and any such additional measures agreed to by the Parties will be documented as an Annex to this DPA or in an Order to the Agreement.

12.2 The Customer further agrees that to the extent that Provider is required to enter into an appropriate transfer mechanism or additional safeguards to transfer Personal Data under applicable Privacy Laws, Provider may enter into an agreement to affect such a transfer on its own behalf, and where required on behalf of the Customer, on a named or unnamed basis.

12.3 Due to the fact that Provider has no control over the type, character, properties, content, and/or origin of Personal Data Processed hereunder, notwithstanding anything to the contrary herein, Provider shall not be in breach of this DPA or the Agreement or liable to Customer to the extent Personal Data subject to jurisdictional requirements mandating security, processing or other measures not set forth in, or contrary to the terms of, this DPA is provided by Customer without amending this DPA or entering into an Order addressing the same.

12.4 If any variation is required to this DPA as a result of a change in Privacy Laws, including any variation which is required to the Standard Contractual Clauses, then either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to this DPA, including the Standard Contractual Clauses, to address such changes.

13. GENERAL TERMS.

13.1 This DPA shall be governed by and construed in accordance with the laws of the State of Delaware and the Parties hereby submit to the courts in the State of Delaware with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

13.2 The applicable law provisions of this DPA are without prejudice to clauses 7 (Mediation and Jurisdiction) and 10 (Governing Law) of the Standard Contractual Clauses where applicable to Restricted Transfers of Personal Data from the European Union (including the United Kingdom) to a third country.

14. ORDER OF PRECEDENCE.

14.1 Nothing in this DPA reduces Provider's or any Provider Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Provider or any Provider Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of inconsistencies between the provisions of this DPA and (i) the Information Security Schedule), or (ii) any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail. For the avoidance of doubt, the limitations and exclusions of liability set out in the Agreement shall also apply in respect of this DPA, to the fullest extent permitted under applicable law.

15. SEVERANCE.

15.1 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX 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) 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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 - Optional

Not used.

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.

MODULE TWO: 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. 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 (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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional

documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

MODULE TWO: Transfer controller to processor

(a) 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 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. 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.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(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.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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;

  (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). [For Module 3: The data exporter shall forward the notification to the controller.]

(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 [For Module 3: if appropriate in consultation with the controller]. 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 [For Module 3: the controller or] 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.

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 3: 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 [For Module 3: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

Governing law

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

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]*

Data Exporter	
Name	Customer as identified in the Agreement
Address	As detailed in the Agreement
Contact person name, position and contact details	As detailed in the Agreement
Activities relevant to the data transferred under these Clauses	Receipt of services under the Agreement
Signature and date	By entering into the Agreement, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein as of the effective date of the Agreement.
Role (controller/processor)	Controller

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

Data Importer	
Name	Provider as identified in the Agreement, being Revalize, Inc or

	such subsidiary thereof as identified in the Agreement
Address	As detailed in the Agreement
Contact person name, position and contact details	Kristen Shaheen, General Counsel & Chief Privacy Officer, Revalize, Inc, Kristen.shaheen@revalizesoftware.com
Activities relevant to the data transferred under these Clauses	Provision of services under the Agreement
Signature and date	By entering into the Agreement, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein as of the effective date of the Agreement.
Role (controller/processor)	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Employees, clients, customers and suppliers of Customer. Employees or contractors of Customer who contact Provider's technical support facilities.
Categories of personal data transferred	Customer's employee categories: name, title, department, ID number, system usage, email address, job title, login credentials and/or contact telephone number. Customer's end-user or consumer categories: name, email address, contact telephone number, account number. Additional Categories of Personal Data may be provided by Customer either as part of a Support request or through Customer's use of Hosted Subscription Services.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and 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.	Not applicable.
The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis)	Support & Professional Services: Personal Data is processed only for as long as is necessary to provide the particular Support and/or Professional Services. Subscription Services: Personal Data is stored for the duration of the Services and is deleted or returned to Customer as set out in the data processing agreement or as otherwise amended or deleted by Customer during the Term.
Nature of the processing	Provider may Process Personal Data as necessary to perform the Services, including where applicable for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing

	system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration,implementation,configuration and performance testing.
Purpose(s) of the data transfer and further processing	Support may be provided by Provider in accordance with Provider's Support Plan. When providing Support, Provider may be required by Customer to Process Personal Data. Provider may access and/or receive Personal Data when providing Support. Personal Data is not accessed and/or received in every Support case because some errors can be analyzed and rectified without such access if the background to the error is known. Depending on the issue, Provider or third-party vendors may provide Support and therefore an international transfer of Personal Data may occur. If, as part of an Order, Customer requires Provider to perform Professional Services to assist in deployment of the product during the term, then Provider may be required by Customer to Process Personal Data as part of that engagement. Customer will upload data to the Hosted Subscription Services in order to maximize the functionality of the product. Some of the data which may be uploaded to the Hosted Subscription Services may include Personal Data. Provider will store (either directly or using a third party Subprocessor as noted below) all data uploaded into the Hosted Subscription Services on behalf of Customer in accordance with the terms and conditions of service under the Agreement as mutually agreed to by the Parties. Customer will determine how and why the product will be used to its benefit which may include the frequent or infrequent use of Personal Data. Customer acknowledges that in relation to these Processing operations, Provider has no control over the submission of Data Subject's Personal Data and that the design of the data to be submitted to Provider's

	Hosted Subscription Services is at all times under the control of Customer. Except for the storage of the data within the Hosted Subscription Services (and the provision of Support, if applicable, described above), Provider is not involved in any Processing activities associated with this use of the product. If, as part of an Order, Customer requires Provider to perform Professional Services to assist in deployment of the product or application managed services during the Term, then Provider may be required by Customer to Process Personal Data for those purposes.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	For as long as necessary to perform the Services.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	The Provider may transfer Personal Data to sub-processor(s) for the purposes of performing the Services for such period as is necessary for such performance.

C. COMPETENT SUPERVISORY AUTHORITY

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

European Economic Area:
The State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg (https://www.baden-wuerttemberg.datenschutz.de)

Switzerland:
The Swiss Federal Data Protection Authority
(https://www.edoeb.admin.ch/edoeb/en/home.html)

United Kingdom:
The Information Commissioner's Office (ICO) (https://ico.org.uk/)

ANNEX II

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

PART 1 – TECHNICAL MEASURES TO ENSURE SECURITY OF PROCESSING

Technical Measures to Ensure Security of Processing	**Description**
1. Inventory and Control of Hardware Assets	Actively manage all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.
2. Inventory and Control of Software Assets	Actively manage all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4. Controlled Use of Administrative Privileges	Maintain processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, applications, and data.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Implement and manage the security configuration of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
6. Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyse audit and security logs of events that could help detect, understand, or recover from a possible attack.
7. Email and Web Browser Protections	Deploy automated controls to minimise the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems or content.
8. Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action.
9. Limitation and Control of Network Ports, Protocols, and Services	Manage (track, control, correct) the ongoing operational use of ports, protocols, services, and applications on networked devices in order to minimise windows of vulnerability and exposure available to attackers.
10. Data Recovery Capabilities	Maintain processes and tools to properly back up personal data with a proven methodology to ensure the

	confidentiality, integrity, availability, and recoverability of that data.
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Implement and manage the security configuration of network infrastructure devices using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
12. Boundary Defenses	Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data.
13. Data Protection	Maintain processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the confidentiality and integrity of personal data.
14. Controlled Access Based on the Need to Know	Maintain processes and tools to track, control, prevent, and correct secure access to critical or controlled assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical or controlled assets based on an approved classification.
15. Wireless Access Control	Maintain processes and tools to track, control, prevent, and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.
16. Account Monitoring and Control	Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimise opportunities for unauthorised, inappropriate, or nefarious use.

PART 2 – SUPPLEMENTARY MEASURES

1. Implement a Comprehensive Information Security Programme	Through the implementation of a Comprehensive Information Security Programme (CISP), maintain various administrative safeguards to protect personal data. These measures are designed to ensure: security, confidentiality and integrity of personal data protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud that employees, contractors, consultants, temporaries, and other workers who have access to personal data only process such data on instructions from the data controller.
2. Implement a Security Awareness and Training Programme	For all functional roles (prioritizing those mission critical to the business, its security, and the protection of personal data), identify the specific knowledge, skills and abilities needed to support the protection and defense of personal data; develop and execute an integrated plan to assess, identify gaps, and remediate

	through policy, organisational planning, training, and awareness programmes.
3. Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
4. Incident Response and Management	Protect the organisation's information, including personal data, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight, retainers, and insurance) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the organisation's network and systems.
5. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises	Test the overall strength of the organisation's defense (the technology, processes, and people) by simulating the objectives and actions of an attacker; as well as, assess and validate the controls, policies, and procedures of the organisation's privacy and personal data protections.
6. Physical Security and Entry Control	Require that all facilities meet the highest level of data protection standards possible, and reasonable, under the circumstances relevant to the facility and the data it contains, process, or transmits.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors: please see the list at https://revalizesoftware.com/legal/

APPENDIX 2

UK ADDENDUM

ICO INTERNATIONAL DATA TRANSFER ADDENDUM TO EU COMMISSION STANDARD CONTRACTUAL CLAUSES (UK)

BACKGROUND

(A) 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.

AGREED TERMS

Table 1: Parties [ICO clause]

Start Date	The commencement date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Customer as identified in the Agreement	Provider as identified in the Agreement
	Trading name (if different):	Trading name (if different):
	As identified in the Agreement	As identified in the Agreement
	Official registration number (if any) (company number or similar identifier): As identified in the Agreement	Official registration number (if any) (company number or similar identifier): As identified in the Agreement
Key contacts	Full name (optional):	Full name (optional): Kristen Shaheen
	Job title: As identified in the Agreement	Job title: General Counsel & Chief Privacy Officer
	Contact details including email: As identified in the Agreement	Contact details including email: kristen.shaheen@revalizesoftware.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	[X] The version of the Approved EU SCCs, which this Addendum is appended to, detailed below, including the Appendix Information. Date: date of the Agreement 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				-	-	

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):

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: [X] Importer [X] Exporter ☐ Neither Party

PART 2: MANDATORY CLAUSES

Entering into this Addendum

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

Interpretation of this Addendum

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

Addendum: This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

Addendum EU SCCS: The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information: As set out in Table 3.

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) of the UK GDPR.

Approved Addendum: The template Addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs: The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

ICO: The Information Commissioner.

Restricted Transfer: A transfer which is covered by Chapter V of the UK GDPR.

UK: The United Kingdom of Great Britain and Northern Ireland.

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

UK GDPR: As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation ((EU) 2016/679), then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    (a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    (b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    (c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    (a) references to the "Clauses" mean 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 1 is replaced with "Clause 11(c)(i)";

(j) Clause 13(a) and Part C of Annex I are not used;

(k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

(l) In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(m) Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

(n) Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

(o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

(a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

(b) reflects changes to UK Data Protection Laws.

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

(a) its direct costs of performing its obligations under the Addendum; and/or

(b) its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

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 section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

APPENDIX 3

SWISS ADDENDUM

This Addendum is intended to amend the EU SCCs to accommodate the Swiss Federal Act on Data Protection ("FADP") in accordance with the decision of the Swiss Data Protection Authority ("FDPIC"). This Addendum applies if and to the extent a transfer of personal data to a country outside the EU or EEA without an adequate level of data protection governed by the SCCs is subject to the FADP. In such cases, the EU SCCs shall be interpreted as follows:

1. References to the General Data Protection Regulation shall be deemed to include references to the equivalent provisions of the FADP.
2. Clause 13 and Annex 1 C shall include the FDPIC as the competent supervisory authority for Switzerland.
3. Clause 17 shall include Swiss law as the governing law where the transfer is exclusively subject to FADP.
4. The term "Member State" shall be extended to include Switzerland for the purposes of allowing Swiss data subjects to pursue their rights in their habitual place of residence.