Signature Page to Attached
Data Processing & Protection Addendum
and
Standard Contractual Clauses

This signature page is a part of and attached to the Data Processing & Protection Addendum including the exhibits, appendices and attachments hereto **("Addendum"),** entered into effective as of latest date set forth below on this page and forms part of the agreement(s) executed between the undersigned parties and/or their affiliates in connection therewith **(**collectively, and as amended, the **"Principal Agreement")** between the customer named below **("Customer")** acting on its own behalf and as agent for each Customer Affiliate; and (ii) **Riverside Assessments, LLC dba Riverside Insights ("Riverside")** acting on its own behalf and as agent for each Riverside Affiliate.

Each of the undersigned represents and warrants that they have read this Addendum, including without limitation, the Standard Contractual Clauses and Appendices 1 and 2 thereto (the "SCCs") and are authorized to execute this Addendum and the SCCs on behalf of the entity named below.

IN WITNESS WHEREOF, each of the undersigned has caused the Addendum and the SCCs to be duly executed, with effect from the date first set out above.

Riverside Assessments, LLC

Signature Scott E. Olson

Name: Scott E. Olson

Title: Manager of Proposal Services

Date Signed: [[2/24/2023]]

Email: contracts@riversideinsights.com

Customer

____

Signature____________________________________

Name______________________________________

Title Date Signed______________________________

Address _____________________________________
____
____

Telephone_____________________________ Email________________

Data Processing & Protection Addendum

Capitalized terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

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

1.1.1 **"Customer Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.1.2 **"Customer Client"** means any entity that engages Customer or a Customer Affiliate to Process Personal Data on its behalf, and whose Personal Data Riverside and/or Riverside Affiliates Processes under the Principal Agreement and this Addendum.

1.1.3 **"Customer Group Member"** means Customer or any Customer Affiliate;

1.1.4 **"Contracted Processor"** means Riverside or a Subcontractor engaged by Riverside to Process Personal Data on Riverside's behalf;

1.1.5 **"Data Protection Laws"** means UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

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

1.1.7 **"UK Data Protection Laws" means the data protection law of the UK which is the UK GDPR and the Data Protection Act 2018 ("DPA 2018").**

1.1.8 **"GDPR"** means UK General Data Protection Regulation;

1.1.9 **"Personal Data"** means any personal data, as such term is defined under applicable Data Protection Laws, which is Processed by or on behalf of Riverside pursuant to or in connection with the Principal Agreement;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1. a transfer of Personal Data from any Customer Group Member to a Contracted Processor; or

1.1.10.2. an onward transfer of Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under Section 6.4.3 or 12 below;

1.1.11 **"Riverside Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Riverside, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise. To the extent a Riverside Affiliate Processes Customer Personal Data in connection with the Services, references in this Addendum to Riverside shall include such Riverside Affiliate;

1.1.12 **"Services"** means the services and other activities to be supplied to or carried out by or on behalf of Riverside for any Customer Group Members pursuant to the Principal Agreement;

1.1.13 **"Standard Contractual Clauses"** means SCCs (UK Controller-to-Processor); and

1.1.14 **"Subcontractor"** means a third party engaged by Riverside to perform Processing activities in connection with Personal Data.

1.2 The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", **"Personal Data Breach", "Processing"** and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word **"include"** shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Roles of Parties and Authority

2.1 Notwithstanding anything to the contrary in the Principal Agreement, Customer and Riverside agree that, for purposes of UK Data Protection Laws and with respect to the Processing of Personal Data by or on behalf of Customer in connection with the provision of the Services under the Principal Agreement and this Addendum:

2.1.1 Customer Client shall be a "Controller;"

2.1.2 Customer Group Members shall each be a "Processor;" and

2.1.3 Riverside and Riverside Affiliates shall each be a "Subprocessor".

2.2 Riverside warrants and represents that, before any Riverside Affiliate Processes any Personal Data in connection with the Services, Riverside's entry into this Addendum as agent for and on behalf of that Riverside Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Riverside Affiliate.

3. Processing of Personal Data

3.1 Riverside shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Personal Data; and

3.1.2 not Process Personal Data other than on the relevant Customer Group Member's documented instructions unless Processing is required by Applicable Laws to Riverside is subject, in which case Riverside shall to the extent permitted by Applicable Laws inform the relevant Customer Group Member of that legal requirement before Processing such Personal Data.

3.2 Each Customer Group Member:

3.2.1 Shall be solely responsible for its own compliance with applicable Data Protection Laws, including ensuring that there is a lawful basis for processing of Personal Data transferred to Riverside pursuant to the Principal Agreement.

3.2.2 Instructs Riverside (and authorises Riverside to instruct each Subcontractor) to:

3.2.2.1. process Personal Data for purposes of providing the Services; and

3.2.2.2. in particular, transfer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Principal Agreement.

3.2.3 Shall ensure that the SCCs to this Addendum set out any and all required information regarding the Processing of the Personal Data as required by GDPR (and, to the extent applicable, equivalent requirements of other Data Protection Laws). In accordance with clause 10 of the SCCs, Customer may make reasonable amendments to the SCCs by written notice to Riverside from time to time as Customer reasonably considers necessary to comply with any applicable Customer Client's reasonable instructions.

4. Riverside Personnel

Riverside shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 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, Riverside shall, in relation to the Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in the GDPR and as set forth in the SCCs.

5.2 In assessing the appropriate level of security, Riverside shall take account in particular of the risks that are presented by Processing of the Personal Data, in particular from a Personal Data Breach.

6. Subcontractors

6.1 Each Customer Group Member authorises Riverside to appoint (and permit each Subcontractor appointed in accordance with this Section 6 to appoint) Subcontractors in accordance with this Section 6 and any restrictions in the Principal Agreement.

6.2 Riverside may continue to use those Subcontractors already engaged by Riverside as of the effective date of this Addendum, subject to Riverside as soon as practicable meeting the obligations set out in Section 6.4.

6.3 Riverside shall give Customer prior written notice of the appointment of any new Subcontractor, including full details of the Processing to be undertaken by the Subcontractor. The appointment of any new Subcontractor shall be subject to the Customer's prior written consent, not to be unreasonably withheld or delayed.

6.4 With respect to each new Subcontractor, Riverside shall:

6.4.1 before the Subcontractor first Processes Personal Data (or, where relevant, in accordance with Section 6.2), carry out adequate due diligence to ensure that the Subcontractor is capable of providing the level of protection for Personal Data required by the Principal Agreement;

6.4.2 ensure that the arrangement between Riverside and the Subcontractor is governed by a written contract which imposes the same obligations on the Subcontractor as are imposed on Riverside as set forth in the SCCs;

6.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between Riverside and the relevant Subcontractor; and

6.4.4 provide to Customer for review such copies of the above referenced agreements (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request in writing from time to time.

6.5 Riverside shall ensure that each Subcontractor performs the applicable obligations under this Addendum, as they apply to Processing of Personal Data carried out by that Subcontractor, as if it were party to this Addendum in place of Riverside.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Riverside shall assist each Customer Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer Group Members' obligations as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Riverside shall:

7.2.1 promptly notify Customer if it, or any Subcontractor, receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and

7.2.2 except as otherwise required by Applicable Laws, not respond, and require that any Subcontractor does not respond, to that request except on the documented instructions of the applicable Customer Group Member. To the extent Riverside and/or any Subcontracor is required, pursuant to Applicable Laws, to respond directly to a request from a Data Subject, Riverside shall promptly notify Customer of such requirement in advance; and

7.2.3 be entitled to reasonable compensation from Customer for Riverside's time and efforts spent in responding to requests under this Section 7.

8. Personal Data Breach

8.1 Riverside shall promptly notify Customer without undue delay upon Riverside or any Subcontractor becoming aware of a Personal Data Breach affecting Personal Data, and shall provide Customer with sufficient information to allow each Customer Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. To the extent known at the time of notification, such notification shall as a minimum:

8.1.1 describe the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

8.1.2 communicate the name and contact details of the Riverside's data protection officer or other contact point where more information can be obtained;

8.1.3 describe the likely consequences of the Personal Data Breach; and

8.1.4 describe the measures taken or proposed to be taken by Riverside to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.2 Riverside shall co-operate with each affected Customer Group Member and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8.3 Unless required by applicable law, Riverside shall not inform any third party of any Personal Data Breach involving Personal Data without first obtaining Customer's prior written consent.

9. Data Protection Impact Assessment and Prior Consultation

Riverside shall provide reasonable assistance to each Customer Group Member 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 of any Customer Group Member by the GDPR or equivalent provisions of any other Data Protection Law, 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, Riverside.

10. Deletion or return of Personal Data

10.1 Subject to Sections 10.2 and 10.3, Riverside shall promptly and in any event within 30 days of the date of expiration or termination of the Principal Agreement (the **"Termination Date"),** delete and procure the deletion of all copies of Personal Data. **"Delete"** means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed.

10.2 Subject to Section 10.3, Customer may in its absolute discretion by written notice to Riverside within 14 days of the Termination Date require Riverside to (a) return a complete copy of all Personal Data to Customer by secure file transfer in such format as is reasonably notified by Customer to Riverside; and (b) delete and procure the deletion of all other copies of Personal Data Processed by or on behalf of Riverside. Riverside shall comply with any such written request within 30 days of the Termination Date.

10.3 Each Contracted Processor may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by Applicable Laws and always provided that Riverside shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Riverside shall provide written certification to Customer that it has fully complied with this Section 10 within 10 days of completion of such compliance, and in any event within 45 days of the Cessation Date.

11. Audit rights

Subject to Sections 11.2 and 11.3, Riverside shall make available to Customer on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer, in relation to the Processing of the Personal Data by or on behalf of Riverside.

11.1 Information and audit rights of Customer only arise under Section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11.2 Customer shall give Riverside reasonable notice of any audit or inspection to be conducted under Section 11.1 and shall use (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Riverside's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Riverside need not give access to its premises for the purposes of such an audit or inspection:

11.2.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.2.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice to Riverside that this is the case before attendance outside those hours begins; or

11.2.3 for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which:

11.2.3.1. Customer reasonably considers necessary because of good faith concerns as to Riverside's compliance with this Addendum;

11.2.3.2. A Customer Client is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory; or

11.2.3.3. Customer reasonably considers necessary due to a change in the scope, nature or location of services provided; where Customer has identified its concerns or the relevant requirement or request in its notice to Riverside of the audit or inspection.

12. Restricted Transfers

12.1 Subject to Section 12.3, Customer (as "data exporter") and Riverside (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer.

12.2 The Standard Contractual Clauses shall come into effect under Section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 Riverside warrants and represents that, before the commencement of any Restricted Transfer to a Subcontractor which is not a Riverside Affiliate, Riverside's entry into the Standard Contractual Clauses under Section 12.1, and agreement to variations to those Standard Contractual Clauses made under Section 13.4.1, as agent for and on behalf of that Subcontractor, will have been duly and effectively authorised (or subsequently ratified) by that Subcontractor.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clause 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the SCCs with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the SCCs.

Order of precedence

13.2 Nothing in this Addendum reduces Riverside's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Riverside to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to Section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal 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 Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Customer may:

13.4.1 by at least 30 (thirty) calendar days' written notice to Riverside from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under Section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Customer gives notice under Section 13.4.1:

13.5.1 Riverside shall promptly co-operate (and ensure that any affected Subcontractors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under Section 6.4.3; and

13.5.2 Riverside shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Customer to protect the Contracted Processors Riverside against additional risks associated with the variations made under Section 13.4.1 and/or 13.5.1.

13.6 If Customer gives notice under Section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

13.7 Neither Customer nor Riverside shall require the consent or approval of any Customer Affiliate or Riverside Affiliate to amend this Addendum pursuant to Section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum 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 UK standard contractual clauses for international transfers from controllers to processors

		Non-legally binding guidance
		This column does not form part of the standard contractual clauses, and is not legally binding on either party
Parties		
Name of the data exporting organisation:		This is the sender of the restricted transfer of personal data (referred to as the exporter). Insert the full legal name: If a sole trader, his/her full name. If a company or limited liability partnership – as formally registered. If a partnership as set out in Partnership Deed. If an unincorporated association, check the establishing document, as to who should enter into this contract.
Address		This is the contact address for the exporter. It may be the registered address but does not need to be. You must include the country.
Telephone		This can be the exporter's general contact telephone number.
Fax		This can be the exporter's general contact fax number. Leave this blank if you do not have a fax.

		Non-legally binding guidance
Email		This can be the exporter’s general contact email address
Other information needed to identify the organisation		For UK companies and limited liability partnerships it is helpful to include the following: A company/limited liability partnership (delete as appropriate) registered in England and Wales/Scotland/Northern Ireland (delete as appropriate). Company number: insert number. For companies outside the UK, if possible it is helpful to include the registration number and country of incorporation. A company number is useful as it can help identify a company even if it has changed its name and address.
	(the data **exporter**”)	
	And	
Name of the data importing organisation:	Riverside Assessments, LLC dba Riverside Insights	This is the receiver of the restricted transfer of personal data (referred to as the importer). Insert the full legal name: If a sole trader, his/her full name. If a company or limited liability partnership – as formally registered. If a partnership as set out in Partnership Deed. If an unincorporated association, check the establishing document, as to who should enter into this contract.

		Non-legally binding guidance
Address	One Pierce Place, Suite 101C, Itasca, IL 60143 Country: United States of America	This is the contact address for the importer. It may be the registered address but does not need to be. You must include the country.
Telephone	(800) 323-9540	This can be the importer’s general contact telephone number.
Fax	N/A	This can be the importer’s general contact fax number. Leave this blank if you do not have a fax.
Email	contracts@riversideinsights.com	This can be the importer’s general contact email address
Other information needed to identify the organisation	State of Delaware File Number: 7039799	For UK companies and limited liability partnerships it is helpful to include the following: A company/limited liability partnership (delete as appropriate) registered in England and Wales/Scotland/Northern Ireland (delete as appropriate). Company number: insert number For companies outside the UK, if possible it is helpful to include the registration number and country of incorporation. A company number is useful as it can help identify a company even if it has changed its name and address.
	(the data **importer**”)	
Clause 1. Definitions	For the purposes of the Clauses: (a)‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’,	A brief overview of these definitions are: “Personal data”

		Non-legally binding guidance
	‘data subject’ and ‘Commissioner’ shall have the same meaning as in the UK GDPR;	Information relating to an identified or identifiable natural person. “Special categories of data” Personal data which relates to an individual’s race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation. “Process/processing” In practice means anything which can be done to data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. “Controller” A natural or legal person which decides the purposes and means of processing data “Processor” A natural or legal person which is responsible for processing personal data on behalf of a controller “Data subject” The individual that personal data relates to. “The Commissioner” The Information Commissioner, as the UK’s independent data protection authority, which we refer to as the ‘ICO’.

		Non-legally binding guidance
	(b) 'the data exporter' means the controller who transfers the personal data;	This is the sender/exporter of the personal data, set out on page 1.
	(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;	This is the receiver/importer of the personal data, set out on page 3. The definition clarifies that the importer should not be in a country covered by UK "adequacy regulations". These are UK regulations confirming that the legal framework in a country (or territory or sector) provides an adequate level of data protection for personal data. Currently, it includes all EEA countries and all countries (territories or sectors) covered by a European Commission "adequacy decision" You do not need to use the standard contractual clauses if the importer is covered by UK adequacy regulations.
	(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;	This is a sub-contractor of the processor, to which the processor has delegated some of its personal data processing services.
	(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;	"Applicable data protection law" means the data protection law of the UK which is the UK GDPR and the Data Protection Act 2018 ("DPA 2018").

		Non-legally binding guidance
	(f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.	This definition is aligned with UK GDPR Art 32, which places obligations on both controllers and processors to keep personal data secure. In brief, this requires security measures that involve policies, processes and people as well as technology. This usually means that: You consider things like risk analysis, organisational policies and physical and technical measures. You take into account additional requirements about the security of your processing. You consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses. Where appropriate, you should look to use measures such as pseudonymisation and encryption. Your measures must ensure the confidentiality, integrity and availability of your systems and services and the personal data you process within them. The measures must also enable you to restore access to and availability of personal data in a timely manner in the event of a

		Non-legally binding guidance
		physical or technical incident. You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures regularly (such as pen testing and testing application security), and undertake any required improvements.
Clause 2. Details of the transfer	The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.	You must fill in Appendix 1 with the details of the restricted transfer (see below). Clause 2 flags that if "special categories of personal data" are being transferred these should be set out, as they receive a higher standard of protection in data protection law.
Clause 3. Third-party beneficiary clause		Clause 3 sets out the rights of data subjects to enforce certain provisions in the standard contractual clauses against the importer and exporter. Data subjects do not sign up to the standard contractual clauses, but they can enforce compliance with particular clauses which are intended to benefit them. The clauses which can be enforced by a data subject are set out below. If a data subject wishes to bring a claim for non-compliance with the standard contractual clauses, it must first try to bring the claim against the exporter. If it is not possible to bring a claim against the exporter, the data subject can try to bring a

		Non-legally binding guidance
		claim against the importer (see Cl 3(2)) If it is not possible to bring a claim against the importer, the data subject can try to bring a claim against a sub-processor (if there is one) (see Cl 3(3)).
3(1)	The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.	Data subjects can enforce the clauses listed directly against the exporter. Data subject enforcement against: ☑ Exporter (if that is not possible:) ☑ Importer (if that is not possible:) ☑ Sub-processor
3(2)	The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.	Data subjects can enforce the clauses listed directly against the importer, but only where: the exporter has "factually disappeared" (for example, it is not contactable or traceable) OR it no longer legally exists (for example, it is a company which has been dissolved); and there is no entity which has taken over all of the exporter's obligations. Data subject enforcement against: ☑ Exporter If that is not possible: ☑ Importer If that is not possible:

		Non-legally binding guidance
		☑ Sub-processor
3(3)	The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.	Data subjects can enforce the clauses set out listed directly against the sub-processor if: both the exporter and importer have either "factually disappeared" (for example, neither is contactable or traceable) OR no longer legally exist (for example: a company which has been dissolved); and there is no entity which has taken on all of the exporter's obligations.
		Data subject enforcement against: ☑ Exporter If that is not possible: ☑ Importer If that is not possible: ☑ Sub-processor
3(4)	The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.	This clause prevents the exporter and importer objecting to data subjects being represented by associations or other bodies (eg interest or campaign groups).
		Data subject enforcement against: ☑ Exporter If that is not possible:

		Non-legally binding guidance
		☑ Importer If that is not possible: ☑ Sub-processor
Clause 4. Obligations of the data exporter	The data exporter agrees and warrants:	Clause 4 sets out the general commitments which the exporter provides in relation to the data. These commitments are “warranties”, which are promises given in a contract. If the exporter does not comply with a warranty, this may lead to a claim from the importer for damages. If the exporter does not comply with certain obligations, this may lead to a claim from data subjects. We have shown below where a data subject can take such action in relation to a clause. These are also set out in Clause 3 above.
4(a)	that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;	The exporter of the data must make sure that it has complied with the UK GDPR and DPA 2018 (and all other UK laws which apply to it), in relation to its collection, use and transfer of the personal data being sent under the standard contractual clauses. The clause refers to notifying the ICO about processing activities. However, exporters in the UK no longer need to notify the ICO of their processing of personal data.
4(b)	that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data	The exporter must only instruct the importer to process the data on the exporter's behalf (i.e. for the purposes instructed by the exporter).

		Non-legally binding guidance
	exporter’s behalf and in accordance with the applicable data protection law and the Clauses;	The instructions must also be: in accordance with the UK GDPR and the DPA 2018; and in accordance with the standard contractual clauses. This means that the exporter cannot instruct the importer to do something which is not permitted by the UK GDPR and DPA 18, or by the standard contractual clauses. Data subject enforcement against: ☑ Exporter
4(c)	that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;	The exporter must ensure that the importer provides sufficient guarantees in relation to the security measures set out by the parties in Appendix 2. In practice, ensuring that the importer provides sufficient guarantees is likely to involve the exporter carrying out due diligence on the importer before it selects it as a processor. This might include: asking questions about the importer’s data protection practices; reviewing its security measures; reviewing its internal data protection policies; and asking questions about any previous data security incidents. Data subject enforcement against: ☑ Exporter

		Non-legally binding guidance
4(d)	that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;	This clause requires the exporter to have assessed the importer's security measures, both technical and organisational (which includes policies, processes and people). The exporter must be satisfied that these security measures offer appropriate protection for the data being transferred, to protect it against it being destroyed, lost, altered or disclosed, or accessed by unauthorised persons. The UK GDPR and the standard contractual clauses do not set any specific mandatory security measures. It is for the exporter to assess what measures are appropriate in the circumstances, taking into account: the nature of the data; the nature of the technology used to process the data; the cost of implementing any particular measures; and the risks that could arise from any accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access to the personal data. The parties should keep the measures under review and be aware that they may need to change or update them over time as new technology becomes available, or if the risks of the processing change.
		Data subject enforcement against: ☑ Exporter

		Non-legally binding guidance
4(e)	that it will ensure compliance with the security measures;	This clause makes the exporter responsible for ensuring that the importer complies with the security measures set out in Appendix 2. This is an on-going obligation which lasts for the duration of the processing by the importer. This means that the exporter should take steps throughout the life of the contract to make sure that the importer is complying with the measures. This could be by asking questions to the importer or by audits of the importer on a regular basis (such as annually). Data subject enforcement against: ☑ Exporter
4(f)	that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;	This clause only applies where special categories of data are transferred to the importer. In that case, the exporter must tell data subjects that their data has been transferred outside the UK to a country not covered by UK adequacy regulations. Data subject enforcement against: ☑ Exporter
4(g)	to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;	This clause relates to circumstances in which the exporter has received one (or both) of the following notifications from the importer. **- A notification under clause 5(b):** that the laws which apply to the importer have changed and this is

		Non-legally binding guidance
		likely to have a substantial adverse effect on the importer’s obligations under the standard contractual clauses. **- A notification under clause 8(3):** telling the exporter about any laws applicable to the importer which prevent an audit by the ICO of the importer or any sub-processor. If the exporter receives such a notification but still plans to continue the transfer of data to the importer or (if it has stopped transferring personal data) to lift a suspension, it must forward the notification to ICO). This is so that the ICO can decide whether to audit the importer to ensure that the personal data is adequately protected.
		Data subject enforcement against: ☑ Exporter
4(h)	to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;	The exporter must provide copies of the following documents/ information to data subjects who request them: the standard contractual clauses (excluding Appendix 2); a summary description of the security measures in Appendix 2; and any contract for sub-processing services which has to be made in accordance with the standard contractual clauses (see clause 11 below which covers using a sub-processor).

		Non-legally binding guidance
		1. The exporter can remove commercial information before disclosing the standard contractual clauses and any sub-processing contract to a data subject. Data subject enforcement: Exporter
4(i)	that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses;	The exporter must make sure that: any sub-processing is carried out in accordance with the requirements of clause 11; and any sub-processor provides at least the same level of data protection and rights of data subjects as the importer is required to provide under the standard contractual clauses. Data subject enforcement against: Exporter
4(j)	that it will ensure compliance with Clause 4(a) to (i).	This clause requires the exporter to ensure its own compliance with clauses 4(a) to 4(i), set out above. In practice, this means that the exporter will need to make sure its employees, contractors and agents comply with clauses 4(a) to 4(i).
Clause 5. Obligations of	The data importer agrees and warrants:	Clause 5 sets out the general commitments which the importer gives in relation to the data.

		Non-legally binding guidance
the data importer[1]		These commitments are “warranties”, which are promises given in a contract. If the importer does not comply with a warranty, this may lead to a claim from the exporter for damages against the importer. In addition, if the importer does not comply with certain obligations, this may lead to a claim from data subjects. We have indicated below where a data subject can take such action in relation to a clause. These are also set out in Clause 3 above. The obligations in Clause 5 are intended to make sure that the importer, who is not subject to the UK GDPR, provides at least the same level of protection for the personal data as required under the UK GDPR.
5(a)	to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;	The importer must process the data: only on behalf of the exporter; and in accordance with the exporter’s instructions. 2. If the importer cannot do this, it must promptly tell the exporter. Following this, the exporter can suspend the transfer of

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

		Non-legally binding guidance
		data to the importer and/or the exporter can terminate the contract.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
5(b)	that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;	This clause requires the importer to consider the laws that apply to it and whether any of those laws will prevent it from meeting the exporter's instructions and complying with its obligations under the standard contractual clauses. If any of the laws which apply to the importer change – and these changes are likely to have a substantial adverse effect on the promises and obligations set out in the standard contractual clauses – the importer must notify the exporter as soon as it becomes aware of the changes. A "substantial adverse effect" would be any legal requirement on the importer which might prevent the importer from complying with the standard contractual clauses. In these circumstances, the exporter can stop the transfer of data to the importer and/or terminate the contract.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible:

		Non-legally binding guidance
		Sub-processor
5(c)	that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;	The importer must put in place the security measures contained in Appendix 2 before it starts processing the data. This effectively means that the security measures must be place before the data is transferred to the importer. The UK GDPR or the standard contractual clauses do not set any mandatory security measures. It is for the exporter to assess what is appropriate in the circumstances. When deciding what security measures are appropriate, the receiver should think about the type of data (eg how sensitive it is), the type of processing carried out (eg how intrusive it is) and the likely harm which could come to data subjects if the data were lost, stolen or accessed by an unauthorised person. Further guidance: ICO: A Practical Guide to IT Security NCSC: Cyber Security: Small Business Guide NCSC: Cyber Essentials Scheme Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
5(d)	that it will promptly notify the data exporter about:	The importer must promptly tell the exporter about:

		Non-legally binding guidance
	(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; (ii) any accidental or unauthorised access; and (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;	any legally binding request for disclosure of the personal data it receives from a law enforcement agency (unless it is prohibited by law from telling the exporter); any accidental, unlawful or unauthorised access to the data; and any request the importer receives directly from a data subject. The importer must not respond to a request from a data subject unless the exporter authorises it to do so.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
5(e)	to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;	The importer must respond promptly to any questions from the exporter about the importer's processing of the data. The importer must also follow the advice of the ICO about the processing of the personal data transferred, as the restricted transfer is from an exporter in the UK.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor

		Non-legally binding guidance
5(f)	at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;	If the exporter requests, the importer must allow the exporter to carry out an audit of the facilities it uses to process the personal data transferred. Audits can be carried out by: the exporter itself; or third party auditors appointed by the exporter. These auditors must be independent and have appropriate professional qualifications. They must also be subject to confidentiality obligations in relation to the data. The appointment of third party auditors does not currently require agreement by the ICO.
5(g)	to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;	The importer must provide copies of the following documents/information to data subjects who request them: the standard contractual clauses (excluding Appendix 2); a summary description of the security measures in Appendix 2; and any existing contract for sub-processing. 3. The importer can remove commercial information from the sub-processing contracts and the standard contractual clauses before disclosing them to a data subject.

		Non-legally binding guidance
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
5(h)	that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;	The importer can only appoint sub-processors to process the personal data if it has told the exporter about this – and the exporter has consented in writing beforehand to this appointment. 4. The authorisation required for appointing sub-processors should be set out in the main contract between the exporter and the importer (under UK GDPR rules on controller-processor contracts). Data subject enforcement: Exporter Importer Sub-processor
5(i)	that the processing services by the sub-processor will be carried out in accordance with Clause 11;	5. The importer must make sure that its sub-processors process the personal data in accordance with clause 11. Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor

		Non-legally binding guidance
5(j)	to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.	6. The importer must promptly provide to the exporter a copy of all sub-processing agreements it enters into under the standard contractual clauses.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
Clause 6. Liability		Clause 6 sets out which parties will be liable for breaches of the standard contractual clauses. It also sets out data subjects' rights to enforce compliance with the standard contractual clauses by both the exporter and importer.
6(1)	The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.	7. If a data subject suffers damage due to a breach of clauses 3 or 11 by any of the exporter, the importer or a sub-processor, the exporter is responsible in the first instance for compensating the data subject.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
6(2)	If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any	As set out against clause 3, above, if there has been a breach of the clauses set out in clauses 3 or 11 by the

		Non-legally binding guidance
	of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.	exporter, importer or any sub-processor, the data subject should try to bring a claim against the exporter first. If the data subject cannot bring a claim against the exporter because the exporter has factually disappeared, no longer exists in law, or is insolvent, the data subject can bring a claim against the importer. This does not apply if a successor entity has taken on all the legal obligations of the exporter by contract or by operation of law. In that case, the data subject should bring a claim against the exporter's successor. Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
6(3)	If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.	As set out in clause 3, if there has been a breach by a sub-processor of clause 3 or 11, the data subject should try to bring a claim first against the exporter and then the importer. This clause explains that: if the data subject cannot bring a claim against the exporter or the importer because they have factually disappeared, no longer exist in law or are insolvent, the sub-processor agrees that the data subject can bring a claim against it for the sub-processor's own breaches.

		Non-legally binding guidance
		This does not apply if a successor entity has taken on all the legal obligations of the exporter or importer by contract or operation of law. In this case, the data subject should bring a claim against the successor.
Clause 7. Mediation and jurisdiction		Clause 7 relates to circumstances in which a data subject can bring a claim against the importer for breach of the standard contractual clauses.
7(1)	The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject: (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner; (b) to refer the dispute to the UK courts.	If a data subject decides to bring a claim against the importer for breach of the standard contractual clauses, the data subject can choose to either: refer disputes to mediation by an independent person or the ICO; or bring a claim in the courts of the UK. 8. The importer must accept the data subject's decision.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
7(2)	The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.	9. This is an acknowledgement by the exporter and importer that: regardless of whether the data subject chooses mediation or a court action, the data subject can still take advantage of any other

		Non-legally binding guidance
		remedies which are available to them under national or international law. Data subject enforcement: Exporter Importer Sub-processor
Clause 8. Cooperation with supervisory authorities	The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.	The exporter must give a copy of the standard contractual clauses to the ICO if the ICO requests it (or if it is required under applicable data protection law).
8(2)	The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.	The ICO can audit the importer and any sub-processor, in the same way as it could audit the exporter. 10. Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
8(3)	The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).	The importer must tell the exporter about any laws which apply to the importer or any of its sub-processors which would prevent the importer/sub-processor from being audited by the ICO. If there are such laws, the exporter can suspend the transfer of data to the importer and/or terminate the contract.
Clause 9. Governing law		The standard contractual clauses are governed by the

		Non-legally binding guidance
	The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely	law of the UK country of the exporter. → **ACTION**: Fill out this section with the law of the UK where the exporter is established. i.e. choose one of "England and Wales", “Scotland” or “Northern Ireland”. Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
Clause 10. Variation of the contract	The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.	The parties must not amend the standard contractual clauses although: - they must fill in the Appendices and governing law in clauses 9 and 11; - they may make changes which are only to make the Clauses make sense in a UK context (as permitted by Paragraph 7(3) & (4) of Schedule 21 DPA 2018). - they may add commercial clauses which don’t contradict the standard contractual clauses. Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
Clause 11. Sub-processing		This clause covers the use of sub-processors by the importer.

		Non-legally binding guidance
		11. A sub-processor is a processor engaged by the importer to carry out processing activities on behalf of the exporter.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
11(1)	The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[2]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.	The importer can only use a sub-processor if the exporter agrees to this in writing beforehand. There should be rules in the main controller-processor contract regarding how the importer appoints a sub-processor, to meet the requirements of the UK GDPR. If the importer uses a sub-processor, it must enter into a written agreement with the sub-processor. This written agreement must include the same obligations for the sub-processor as those which apply to the importer under the standard contractual clauses. In practice, many importers meet this requirement by having the sub-processor co-sign the standard contractual clauses between the exporter and the importer.

[2] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

		Non-legally binding guidance
		Alternatively, many importers meet this requirement by entering into a duplicate with the sub-processor (i.e. entering into a copy of the same standard contractual clauses as the importer and exporter have signed). 12. If a sub-processor does not comply with its equivalent contractual obligations, the importer remains liable to the exporter for this. It is therefore in the importer's interests to choose its sub-processors carefully.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
11(2)	The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.	The contract between the importer and the sub-processor must include rights for data subjects to bring claims against the sub-processor if: both the exporter and importer no longer exist in law (eg a company which has been dissolved), have factually disappeared (for example, they are uncontactable or traceable) or are insolvent; and no entity has taken on all of the exporter's obligations (in which case the data subject may bring action

		Non-legally binding guidance
		against that successor entity). 13. Claims by data subjects against a sub-processor are limited to damages caused by sub-processor's own processing activities. Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
11(3)	The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.	The agreement between the importer and the sub-processor must be governed by the same law as the standard contractual clauses, set out in Clause 9 above. 14. Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
11(4)	The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.	The exporter must keep a list of sub-processing agreements which the importer has: entered into in relation to the data which is being transferred under the standard contractual clauses; and has told the exporter about. The exporter must update this list at least once a year.

		Non-legally binding guidance
		The exporter must provide this to the ICO if the ICO requests it.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
Clause 12. Obligation after termination		15. Clause 12 sets out obligations under the standard contractual clauses which the parties must still comply with even after the contract has ended, and the importer is no longer providing the data processing services.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
12(1)	The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.	On termination of the data processing services, the importer and all sub-processors must either return all the personal data to the exporter or destroy it. It is up to the exporter to choose whether the data should be returned or destroyed. If the exporter chooses for the importer and sub-processors to destroy the data, the importer and sub-processors must confirm in writing to the

		Non-legally binding guidance
		exporter that they have done this. If laws which apply to the importer/sub-processor mean that they cannot destroy or return the data, they must keep the data confidential and not process it in any other way. The importer is responsible for making sure its sub-processors do this.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
12(2)	The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.	The exporter can audit the importer and the sub-processor to check that they have destroyed the personal data and/or kept it confidential after its processing activity for the exporter has come to an end. 16. The ICO can also audit the importer and the sub-processor to check that they have destroyed this data after its processing activity for the exporter has come to an end.
		Data subject enforcement against: Exporter If that is not possible: Importer If that is not possible: Sub-processor
Indemnification	Please click in the box if you wish to include the following optional clause: ☐ **Include**	This indemnification clause is included an example of an

		Non-legally binding guidance
	Liability The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon: (a) the data exporter promptly notifying the data importer of a claim; and (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.	additional clause which you could include. This example is optional – you do not need to include it, and you can choose to add other additional commercial clauses instead of, or in addition to, this example. You can also amend this example. The clause is a mutual indemnity: the importer indemnifies the exporter; and the exporter indemnifies the importer; if either of them is in breach of the standard contractual clauses. In this context, an “indemnity” means that the party in breach has to fully compensate the other for its losses which arise from its breach. This may be more than just a standard claim for breach of contract, where damages can be claimed. This clause provides a route for an innocent party to claim back from the other any compensation it has had to pay to a data subject under the standard contractual clauses, arising from a breach by that other party. This example indemnity is wider than that, and provides additional compensation for any breach of the standard contractual clauses. Indemnities are often dealt with in the main controller – processor contract between the parties.

		Non-legally binding guidance
Priority of standard contractual clauses	Please click in the box if you wish to include the following optional clause: ☐ **Include** The Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Clauses are entered into. Unless the Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Clauses are entered into, will amend the terms or the effects of the Clauses, or limit any liability under the Clauses, and no term of any such other agreement should be read or interpreted as having that effect.	This clause is provided as it may also be helpful to you. Please review it carefully and only include it if you think it is appropriate for your circumstances. The intended effect of the clause is to make sure that you and the other party do not inadvertently amend the standard contractual clauses or limit your liability. If you did, then you would risk not being able to rely on the standard contractual clauses for compliance with the UK GDPR rules on restricted transfers. The clause allows you the freedom to amend the standard contractual clauses, but only if you expressly refer to them. If you are going to amend the standard contractual clauses, we would always recommend you seek professional legal advice. Any amendment runs the risk that the standard contractual clauses will not comply with the UK GDPR rules on restricted transfers.
On behalf of the data exporter: Name (written out in full): Position:	→ **ACTION**: The exporter should fill in this section with the: Full name of the person signing. This must be a person who is authorised to enter into contracts on behalf of the exporter. Their position. Their business addresses. And sign where indicated.	

	Non-legally binding guidance
Address: Other information necessary in order for the contract to be binding (if any): Signature:	
On behalf of the data importer: Name (written out in full): Scott Olson Position: Manager of Proposal Services Address: One Pierce Place, Suite 101C, Itasca, IL 60143 Other information necessary in order for the contract to be binding (if any): Signature: Scott E. Olson	→ **ACTION**: The importer should fill in this section with the: Full name of the person signing. This must be a person who is authorised to enter into contracts on behalf of the importer. Their position. Their business addresses. And sign where indicated.
Date of the Standard Contractual Clauses:	Do not date the standard contractual clauses until both the exporter and importer have signed. It can be the date of the last signature, or a later date if that is agreed by the exporter and importer.

	Non-legally binding guidance
Appendix 1	
This Appendix forms part of the Clauses and must be completed and signed by the parties.	→ **ACTION**: This Appendix must be appropriately completed for the standard contractual clauses to be an appropriate safeguard and allow restricted transfers of personal data under the UK GDPR. Currently, the UK does not require any additional information to be included in the Appendix. <u>Instructions for using the checklists:</u> To help you completing this Appendix, we have provided optional checklists. These are just suggestions. You do not need to use the checklists at all. You can also amend the contents of any category, as you consider best reflects the international transfer of personal data, including to add specific details. If you do not fit into any of these types, you may add your own description at the end of the checklist.
Data exporter	
The data exporter is (please specify briefly your activities relevant to the transfer): *Please select one option:* ☐ <u>Option 1</u>: The data exporter is (please specify briefly your activities relevant to the transfer): **The data exporter is using the personal data which is being transferred for the following purposes or activities:** The data exporter is using the personal data which is being transferred for the following purposes or activities:	→ **ACTION**: Set out the exporter's type of business and its activities relevant to the restricted transfer. You have two options: <u>Option 1</u>. You may set this out in your own words. As a suggestion, you could use the following form: **The data exporter is:** insert description of importer.

Standard business activities, which apply to most businesses and organisations

☐ Staff administration, including permanent and temporary staff, including appointment or removals, pay, discipline; superannuation, work management, and other personnel matters in relation to the data exporter’s staff.

☐ Advertising, marketing and public relations of the data exporter’s own business or activity, goods or services.

☐ Accounts and records, including

- keeping accounts relating to the data exporter’s business or activity;
- deciding whether to accept any person or organisation as a customer;
- keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;
- keeping customer records
- records for making financial or management forecasts; and
- other general record keeping and information management.

Other activities:

☐ Accounting and auditing services

☐ Administration of justice, including internal administration and management of courts of law, or tribunals and discharge of court business.

☐ Administration of membership or supporter records.

☐ Advertising, marketing and public relations for others, including public relations work, advertising and marketing, host mailings for other organisations, and list broking.

☐ Assessment and collection of taxes, duties, levies and other revenue

☐ Benefits, welfare, grants and loans administration

☐ Canvassing, seeking and maintaining political support amongst the electorate.

☐ Constituency casework on behalf of individual constituents by elected representatives.

☐ Consultancy and advisory services, including giving advice or rendering professional services, and the provision of services of an advisory, consultancy or intermediary nature.

☐ Credit referencing, including the provision of information by credit reference agencies relating to the financial status of individuals or organisations on behalf of other organisations

☐ Data analytics, including profiling

Non-legally binding guidance

The data exporter’s activities which are relevant to the restricted transfer are: add activities.

For example:
"The data exporter is a UK-based supplier of home office equipment and is contracting with the importer for it to provide a software solution for managing the exporter's customer database".

You should also have a controller-processor contract in place. If so, you may be able to re-use a description of the exporter’s activities as set out in that contract.

Option 2: you may find it easier to use the checklists provided.

Instructions:
Step 1: Think about the exporter’s type of business or organisation and click in the box next to the appropriate category, making any appropriate amendments or adding specific detail.

Step 2: Think about why the exporter is using the personal data to be transferred and why it is making the transfer. Click in the box next to all of the activities which apply, making appropriate amendments or adding specific details. You can click “other” and add your own description at the end.

	Non-legally binding guidance
☐ Debt administration and factoring, including the tracing of consumer and commercial debtors and the collection on behalf of creditors, and the purchasing of consumer or trade debts from business, including rentals and instalment credit payments. ☐ Education, including the provision of education or training as a primary function or as a business activity. ☐ Financial services and advice including the provision of services as an intermediary in respect of any financial transactions including mortgage and insurance broking ☐ Fundraising in support of the objectives of the data exporter ☐ Health administration and services, including the provision and administration of patient care. ☐ Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases. ☐ Insurance administration including the administration of life, health, pensions, property, motor and other insurance business by an insurance firm, an insurance intermediary or consultant ☐ IT, digital, technology or telecom services, including use of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software ☐ Journalism and media, including the processing of journalistic, literary or artistic material made or intended to be made available to the public or any section of the public. ☐ Legal services, including advising and acting on behalf of clients. ☐ Licensing and registration, including the administration of licensing or maintenance of official registers. ☐ Not-for-profit organisations’ activities, including • establishing or maintaining membership of or support for a not-for-profit body or association, and • providing or administering activities for individuals who are either members of the not-for-profit body or association or have regular contact with it. ☐ Pastoral care, including the administration of pastoral care by a vicar or other minister of religion. ☐ Pensions administration, including the administration of funded pensions or superannuation schemes. ☐ Procurement, including deciding whether to accept any person or organisation as a supplier, and the administration of contracts, performance measures and other records.	

	Non-legally binding guidance
☐ Private investigation, including the provision on a commercial basis of investigatory services according to instruction given by clients ☐ Property management, including the management and administration of land, property and residential property, and the estate management of other organisations. ☐ Realising the objectives of a charitable organisation or voluntary body, including the provision of goods and services in order to realise the objectives of the charity or voluntary body. ☐ Research in any field, including market, health, lifestyle, scientific or technical research. ☐ Security of people and property, including using CCTV systems for this purpose. ☐ Trading/sharing in personal information, including the sale, hire, exchange or disclosure of personal information to third parties in return for goods/services/benefits. ☐ Other activities (please provide details):	
Data importer	
The data importer is (please specify briefly your activities relevant to the transfer): *Please select one option:* ☑ Option 1: The data importer is (please specify briefly your activities relevant to the transfer): The data importer is a US based company that provides learning, assessment and professional services platforms. The data importer's activities which are relevant to the restricted transfer are: The data importer processes information of data subjects who register to use the data importer's platforms in order to activate and administer user accounts, to provide users with the content and features available through the applicable platform; to communicate with users about the applicable subscription account or transactions with the data importer, and to send information about the platform's features and, where applicable, changes to these features; to personalize the platform's content and experiences for users of the platform. **The data importer's activities for the data exporter, which are relevant to the transfer are:** ☐ Accounts and records services, including • keeping accounts; • deciding whether to accept any person or organisation as a customer	→ **ACTION**: Set out the importer's type of business and its activities relevant to the restricted transfer. You have two options: Option 1. You may set this out in your own words. As a suggestion, you could use the following form: **The data importer is:** insert description of importer. **The data importer's activities which are relevant to the restricted transfer are:** add activities. For example: "The data importer is a US-based supplier of software solutions. It is supplying a software package to the exporter and will host the importer's customer data on its servers in the US."

	Non-legally binding guidance
• keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter; • records for making financial or management forecasts • other general records and information management services. ☐ Administration services relating to membership or supporter records. ☐ Advertising, marketing, and public relations services. ☐ Auditing services ☐ Facilities management services, including cleaning, catering, reception, security, maintenance, gardening, events management, business travel, meetings, vehicle hire, copying, printing and post services. ☐ Benefits, grants and loans administration services. ☐ Consultancy and general advisory services. ☐ Debt administration and factoring services, including the tracing of consumer and commercial debtors and the collection on behalf of creditors. ☑ Education or training services. ☐ Financial services administration and advice services including the provision of services as an intermediary in respect of any financial transactions including mortgage and insurance broking. ☐ Fundraising services. ☐ Health administration and health services, including the provision and administration of patient care. ☐ Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases. ☐ Insurance administration including the administration of life, health, pensions, property, motor and other insurance business. ☑ IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing ☐ Legal administration and legal support services. ☐ Licensing and registration services, including the administration of licensing or maintenance of official registers. ☐ Media services. ☐ Pensions administration, including the administration of funded pensions or superannuation schemes.	You should also have a controller-processor contract in place. If so, you may be able to re-use a description of the importer's activities as set out in that contract. Option 2: you may find it easier to use the checklists provided. Instructions: Step 1: Think about the importer's type of business or organisation and click in the box next to the appropriate category, making appropriate amendments or adding specific detail. Step 2: Think about why the data importer is using the personal data to be transferred. Click in the box next to all of the activities which apply, making appropriate amendments or adding specific details. You can click "other" and add your own description at the end.

	Non-legally binding guidance
☐ Property management services, including the management and administration of land, property and residential property, and the estate management of other organisations. ☐ Procurement services, including deciding whether to accept any person or organisation as a supplier, and the administration of contracts, performance measures and other records. ☐ Provision of temporary and agency staff. ☐ Research and development services, including market, health, lifestyle, scientific or technical research. ☐ Services in relation to the assessment and collection of taxes, duties, levies and other revenue. ☐ Services in relation to trading/sharing in personal information, including the sale, hire, exchange or disclosure of personal information to third parties in return for goods/services/benefits. ☐ Staff administration services, including appointment or removals, pay, discipline; superannuation, training, employee benefits, work management, and other personnel matters in relation to the data exporter's staff. ☐ Other services (please provide a description):	
Data subjects	
The personal data transferred concern the following categories of data subjects (please specify): Current, former and potential data subjects include students, parents/guardians of students, teachers, test takers, administrators and staff. Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff. ☑ staff including volunteers, agents, temporary and casual workers ☑ customers and clients (including their staff) ☐ suppliers (including their staff) ☐ members or supporters ☐ shareholders ☑ relatives, guardians and associates of the data subject ☐ complainants, correspondents and enquirers; ☐ experts and witnesses ☐ advisers, consultants and other professional experts	→ **ACTION**: The parties should list the categories of data subject. Instructions: Think about who the personal data being transferred is about, and click in the box next to all of the categories of data subjects which are included in the personal data being transferred. You may make appropriate amendments or add specific details to any of the categories or click "other" and add your own categories at the end.

	Non-legally binding guidance
☐ patients ☑ students and pupils ☐ offenders and suspected offenders ☐ other (please provide details of other categories of data subjects):	
Categories of data	
The personal data transferred concern the following categories of data (please specify): *Examinees*: first, middle, and last name, date of birth, age, sex, scored reports, grade level, enrollment date, teacher, school of enrollment, school building, funding status, race/ethnicity, language information (native, preferred or primary language spoken), free/reduced lunch status, IEP/IFSP status, student ID number, assessment scores and results, observation data. *Parents/Guardians*: first and last name, email. *Staff*: first and last name, email address, school/building, user name/ID, role/permission, IP addresses, use of cookies, other application technology meta data, meta data on user interaction with application, online communication with customer support. The following is a list of standard descriptions of categories of data: ☑ Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description. ☐ Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details. ☑ Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organisations. ☑ Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records. ☐ Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records,	→ **ACTION**: The parties should list the categories of personal data being transferred. <u>Instructions:</u> Think about <u>what</u> the personal data being transferred is about and click in the box next to all of the categories of personal data which are being transferred You may make appropriate amendments or add specific details to any of the categories, or click "other" and add your own categories at the end.

	Non-legally binding guidance
health and safety records, performance appraisals, training records, and security records. ☐ Financial details, including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information. ☐ Goods or services provided and related information, including details of the goods or services supplied, licences issued, and contracts. ☐ Personal data relating to criminal convictions and offences ☐ Other (please provide details of other data subjects):	
Special categories of data (if appropriate)	
The personal data transferred concern the following special categories of data (please specify): Ethnicity or race, medical information Personal data which is on, which reveals, or which concerns: ☑ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data (if used to identify a natural person) ☑ health ☐ sex life or sexual orientation ☐ criminal convictions and offences ☐ none of the above	→ **ACTION**: Include a list of any of the special categories of data which are being transferred: For completeness, and to ensure the Clauses work under the UK GDPR, we have included the new special categories of data added by the UK GDPR and criminal convictions and offences data. Instructions: Think about the set of personal data being transferred and click in the box next to any of the special categories of data or criminal records and convictions data, which are included.
Processing operations	
The personal data transferred will be subject to the following basic processing activities (please specify): The data importer's activities which are relevant to the restricted transfer are: The data importer processes information of data subjects who register to use the data importer's platforms in order to activate and administer user accounts, to provide users with the content and features available through the applicable platform; to communicate with users about the applicable subscription account or transactions with the data importer, and to send information about the platform's features	→ **ACTION**: List the processing activities which may be carried out. Instructions: Think about how the data importer will be using and handling the set of personal data transferred to it, and click in the box next to all of the

	Non-legally binding guidance
and, where applicable, changes to these features; to personalize the platform’s content and experiences for users of the platform. ☑ Receiving data, including collection, accessing, retrieval, recording, and data entry ☑ Holding data, including storage, organisation and structuring ☑ Using data, including analysing, consultation, testing, automated decision making and profiling ☑ Updating data, including correcting, adaptation, alteration, alignment and combination ☑ Protecting data, including restricting, encrypting, and security testing ☑ Sharing data, including disclosure, dissemination, allowing access or otherwise making available ☑ Returning data to the data exporter or data subject ☑ Erasing data, including destruction and deletion ☐ Other (please provide details of other types of processing):	processing activities which apply. You may make appropriate amendments or add specific details to any of the categories, or click “other” and add your own categories at the end.

DATA EXPORTER Name: Authorised Signature …	→ **ACTION**: The exporter should fill in this section with the: Full name of the person signing. This must be the same person throughout the document. Their position. Their business addresses. **And sign where indicated**.

DATA IMPORTER Name: Scott Olson Authorised Signature … Scott E. Olson	→ **ACTION**: The importer should fill in this section with the: Full name of the person signing. This must be the same person throughout the document. Their position. Their business addresses. **And sign where indicated**.

Appendix 2

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please click in a box to select one option:

☑ Option 2: The following is the description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

- **Encryption of personal data to protect data during transmission and during storage:** All personal data is encrypted at-rest using AES-256-bit encryption and in-transit using a TLS 1.2 cryptographic protocol.

- **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:** Data importer engages a third-party vendor to perform annual penetration testing on its application systems. This testing involves a battery of attacks against customer-facing websites, and the vendor provides detailed reporting at the conclusion of testing. Data importer promptly remediates any vulnerabilities identified in this testing according to the level of severity. Data importer's hosting provider maintains backups of data to accommodate rapid recovery of recent data, as well as for long-term off-site storage. Backups are stored in a secure location within each data center, and the hosting provider follows a security procedure for sending backups to secure offsite locations for long-term storage. All servers and databases are backed up on a regular basis, including differential backups several times daily, weekly full database backups, and full monthly backups (of database and operating system). Backups are monitored daily by staff to ensure successful completion and replication to the designated storage sites.

- **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:** As necessary, data importer's hosting provider will restore any files or directories as requested. The time for restoration varies depending on the size of the files and length of time since deletion. In the event of a catastrophic failure, the database backups will be made available through file transfer that can be delivered to a secondary hosting facility where system functionality would be restored within hours.

- **Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing:** Data importer's assessment platform undergoes annual SOC 2 Type 2 auditing by a reputable third-party. In addition to the annual audit, data importer conducts annual

Non-legally binding guidance

→ **ACTION**: The parties should fill in Appendix 2 with details of the security measures which the importer will provide for the transferred data.

You should also have a controller-processor contract in place, this is often the main service contract you have between you. If so, you may refer to or re-use the importer's security measures set out in that contract.

There are 3 main options for completing this Appendix.

Option 1: simply add in the name and date of the main service contract, to refer to the description of the importer's security measures contained in that agreement.

Option 2: insert your description of the importer's security measures there. You may choose to copy all or part of this from the main service contract.

Option 3: complete the checklist, adding in additional details which are relevant.
Instructions:
The checklist includes the baseline security measures that any business (small or large) should implement to protect its data/systems.

It is unlikely to be appropriate if the data importer is providing IT, digital, technology or telecom processor services.

This checklist for use where the transfer to the data importer and its processing of the personal data does not cause a penetration tests against the production infrastructure on an annual basis by a qualified external party. Vulnerabilities are assigned a vulnerability rating that dictates a timeframe for remediation and are tracked through the internal ticketing system. Finally, data importer's legal and compliance personnel evaluate technical and organisational measures on an ongoing basis and track areas of improvement using a compliance backlog.

- **Measures for user identification and authorisation:** Data importer has policies and procedures for grant access to electronic personal data. Documented authorization is required to grant employees and contractors access to technologies supporting the production environment. These credentials are removed once access is no longer required for the employee or contractor. Data importer follows Role-Based Access Control ("RBAC") to enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. Through RBAC, data importer (i) assigns privileges to individuals based on job classification and function, (ii) restricts access based on a user's need to know, and (iii) is set to "deny all" unless specifically allowed.

- **Measures for ensuring physical security of locations at which personal data are processed:** The production facilities are maintained by third-party hosts' data centers and are hosted within SSAE16 SOC 2 Type 2 audited hosting centers. The production systems computer rooms at these facilities are designed from the ground up to minimize risk of power and climate control failure. All our hosting providers perform periodic testing and auditing of their facilities. All facilities have full battery and generator power. Thus, in the event of an outage, power is maintained indefinitely. All production systems are fully protected by UPS systems and emergency power generators. Data importer has a written contract with its third-party hosting provider that address the latter's notification obligations in the event of a security incident or breach at the data center.

- **Measures for ensuring events logging:** Data importer maintains a robust logging system using a solution provided by Netwrix. These logs record all critical system activity data, including all internet activity passing through the firewall; all web pages, URLs, and objects access on or by the webservers; key transactions within the platform, such as login password fail attempts and the addition and deletion of users; and exceptions and other unusual activity on the database servers. Audit logs are retained for 6 months.

- **Measures for ensuring system configuration, including default configuration:** System configurations are evaluated as part of the annual SOC 2 Type 2 audit. Among other things, third-party auditor confirmed that the platform's configuration ensures that it monitors the internal health of the production infrastructure and that periodic external availability checks are performed for the system. All components of the server infrastructure are deployed using high availability configurations.

particularly high risk to the rights of individuals. For example, where the personal data transferred is:

not special category data;

not criminal convictions and offences data;

not personal details issued as an identifier by a public authority;

not bank account, credit card or other payment data; and

not a large volume of data.

Consider each statement, and the relevant guidance set out below, and click in the box next to those statements which apply.

Add supplementary notes to provide any further relevant detail of those security measures.

Further guidance:

A Practical Guide to IT Security

Cyber Security: Small Business Guide

Cyber Essentials Scheme

Appendix 2

Non-legally binding guidance

- **Measures for ensuring data minimisation:** Data importer's assessment platform only collects, retains, and processes that personal data which is necessary for the delivery of assessment administration, scoring, and reporting services. Customers' assessment needs vary and change, so there are optional data fields that will not impede the delivery of services if they are not provided. Use of such fields up left to each individual customer's discretion.

- **Measures for ensuring data quality:** Data importer maintains process for customers and data subjects to update, correct, and delete personal information. Many of these changes can be made by account holders directly through features within the platform. In addition, data importer's customer support personnel are available to assist authorized representatives of a customer in correcting, updating, and deleting their information.

- **Measures for ensuring limited data retention:** Data importer maintains a records retention and destruction policy that ensures data is not retained beyond the periods necessary for the delivery of services and compliance with applicable legal requirements and the needs of customers and data subjects. Data importer's enterprise risk management council reviews this policy on at least an annual basis and whenever there is a material change in the company's operations.

- **Measures for ensuring accountability:** Data importer explains its data collection, processing, and retention activities in its publicly posted privacy policy. Data importer also evaluates its ability to demonstrate compliance with data privacy laws, including GDPR's core principles, by undergoing annual SOC 2 Type 2 auditing. The Data Privacy Officer is integrated within the organization's decision-making structure and leads data importer's enterprise risk management council.

- **Measures for allowing data portability and ensuring erasure:** Upon request, data importer will assist a customer's authorized representative in exporting data in a readable format (e.g., csv file). With respect to erasure, data importer honors data deletion requests from authorized data subjects and sets forth this process in its data deletion and retention policy.

DATA EXPORTER
Name:
Authorised Signature …

→ **ACTION**: The exporter should fill in this section with the:

Full name of the person signing. This must be the same person throughout the document.

And sign where indicated.

DATA IMPORTER
Name: Scott Olson
Authorised Signature …

→ **ACTION**: The importer should fill in this section with the:

Scott E. Olson	Full name of the person signing. This must be the same person throughout the document. **And sign where indicated**