Data Processing Addendum

Effective 9th December 2020 or if later the date of Processor's receipt of a valid and fully executed version (the "Effective Date")

This Data Processing Addendum forms part of the current agreement(s) or other written or electronic agreement(s) between the Processor and Customer for the purchase of on premises products and online products/services (as more fully set out in the Products/Services Schedule) and as applicable to the Customer's Account with the Processor (the **"Agreement(s)"**) to reflect the parties' agreement with regard to the Processing of Personal Data with effect from the Effective Date.

Upon signing this Data Processing Addendum, the Customer agrees to the terms and conditions herein on behalf of itself and, to the extent required under Applicable Data Protection Law, in the name and on behalf of its Authorized Affiliates, if and to the extent that Processor processes Personal Data for which such Authorized Affiliates qualify as the Controller. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Processor under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates. For the avoidance of doubt, where any natural person, legal entity or organisation signing this DPA is not a current Customer, this Data Processing Addendum is not valid and is not legally binding.

Subject to the parties to the Agreement(s) (which shall remain unchanged), this Data Processing Addendum is entered between:

Party 1	**Party 2**
(i) Wolters Kluwer (UK) Limited, a company registered in England and Wales with company registration number 00450650 having its registered office at 145 London Road, Kingston upon Thames, Surrey, KT2 6SR; **OR** **(ii) Wolters Kluwer (Ireland) Limited**, a company registered in Ireland with company registration number 137230 having its registered office at Ferry House, Mount Street Lower, Saint Peter's, Dublin. (hereinafter to be referred to as "**the Processor**")	the **Customer**, whose details are recorded in the signature box on page 10. (hereinafter to be referred to as the "the **Controller**"),
hereinafter jointly also to be referred to as the **"Parties"** and each separately as a **"Party"**;	

NOW, THEREFORE, and in order to enable the Parties to carry out their relationship in a manner that is compliant with law, the Parties have entered into this Data Processing Addendum as follows:

1. Definitions

For the purposes of this DPA:

"Affiliates"	shall mean any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the outstanding voting securities or capital stock of such subject entity or any other comparable equity or ownership interest with respect to a business entity other than a corporation OR as defined in section 1124 of the Corporation Tax Act 2010;
"Authorised Affiliates"	shall mean any of Customer's Affiliate(s) which (i) is subject to the Applicable Data Protection Law and (ii) is permitted to use the on premises products and/or online products/services pursuant to the Agreement(s) between Customer and the Processor, but has not signed its own Agreement(s) with the Processor and is not a "Customer" in its own right as defined under the Agreement(s).
"**Applicable Data Protection Law**"	shall mean all applicable data protection and privacy legislation in force from time to time in the UK concerning the Processing of Personal Data, including GDPR and the Data Protection Act 2018 applicable to the Controller and the Processor, and additional rules and implementations of EU data protection laid down in European member state or UK law;
"**Controller**"	shall mean Customer and its Authorized Affiliates (as applicable) who determines as a natural or legal person alone or jointly with others the purposes and means of the Processing of Personal Data;
"Customer"	shall mean the other party to the Agreement(s) (not being a Wolters Kluwer group company) that purchased the Services from the Processor;
"Customer's Account"	shall mean the Customer's account with the Processor (as applicable) which records all Services purchased by the Customer under the Agreement(s) as at the Effective Date;
"Customer Account Data"	shall mean Personal Data that relates to Customer's relationship with the Processor, including the names and/or contact information of individuals authorized by Customer to discuss account

	information, billing and support information or of individuals that Customer has associated with obtaining the Processor's Services;
"DPA"	shall mean this Data Processing Addendum;
"**General Data Protection Regulation**" or "**GDPR**"	shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data which will come into effect on May 25, 2018;
"International Organization"	shall mean an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
"**Member State**"	shall mean a country belonging to the European Union;
"**Personal Data**	shall mean any information relating to an identified or identifiable natural person (Data Subject);
"**Data Subject**"	shall mean an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
"**Personal Data Breach**"	shall mean a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorized disclosure or, or access to, Personal Data transmitted, stored or otherwise Processed;
"**Process/Processing**"	shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"**Processor**"	shall mean one of the entities listed under Party 1 above, who Processes Personal Data on behalf of the Controller;
"**Services Agreement**"	shall mean all Agreement(s) concluded between the Controller and the Processor setting out the terms and conditions for the provision of the Services;

"**Services**"	shall mean the services provided by the Processor to the Controller and described under 'subject matter of processing' in the Products/Services Schedule of this DPA;
"**Special Categories of Data**"	shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data, biometric data Processed for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation;
"**Sub-processor**"	shall mean any data processor engaged by the Processor who agrees to receive from the Processor Personal Data exclusively intended for Processing activities to be carried out on behalf of the Controller in accordance with its instructions, the terms of this DPA and the terms of a written subcontract;
"**Supervisory Authority**"	shall mean an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;
"**Technical and Organizational Security Measures**"	shall mean those measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing;
"Third Country"	shall mean a country where the European Commission has **not** decided that the country, a territory or one or more specified sectors within that country, ensures an adequate level of protection; and
"Wolters Kluwer group"	shall mean the Processor and its Affiliates engaged in the Processing of Personal Data.

2. Details of the Processing

The parties acknowledge and agree that with regard to the Processing of Customer Account Data Customer is a controller or processor, as applicable, and one of the entities listed under Party 1 is an independent controller, not a joint controller with Customer. Each party shall comply with its obligations under the Applicable Data Protection Law.

The details of the Processing operation provided by the Processor to the Controller as a commissioned data processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Annex 1 in respect of on premises products and online products/services to this DPA. The Services Agreement and this DPA sets out Controller's complete instructions to Processor in relation to the Processing of the Personal Data and any Processing required outside of the scope of these instructions will require prior written agreement between the parties.

3. Rights and Obligations of Controller

The Controller:

(a) remains the responsible data controller for the Processing of the Personal Data as instructed to the Processor based on the Services Agreement, this DPA and as otherwise instructed. The Controller has instructed and throughout the duration of the commissioned data processing will instruct the Processor to Process the Personal Data only on Controller's behalf and in accordance with the Applicable Data Protection Law, the Services Agreement, this DPA and Controller's instructions. The Controller is entitled and obliged to instruct the Processor in connection with the Processing of the Personal Data, generally or in the individual case. Instructions may also relate to the correction, deletion, blocking of the Personal Data. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by the Controller in writing without delay. To the extent that the implementation of an instruction results in costs for the Processor, the Processor will first inform the Controller about such costs. Only after the Controller's confirmation to bear such costs for the implementation of an instruction, the Processor is required to implement such instruction.

(b) warrants that:

(i) its processing of the Personal Data is based on legal grounds for processing as may be required by Applicable Data Protection Law and it has made and shall maintain throughout the term of the Services Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by Applicable Data Protection Law with respect to Processor's processing of Personal Data under this DPA and the Services Agreement;

(ii) it is entitled to and has all necessary rights, permissions and consents to transfer the Personal Data to Processor and otherwise permit Processor to process the Personal Data on its behalf, so that Processor may lawfully use, process and transfer the Personal Data in order to carry out the Services and perform Processor's other rights and obligations under this DPA and the Services Agreement. Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data; and

(iii) it has assessed the Technical and Organizational Measures set out in Annex 4 of this DPA and has determined that these satisfy the requirements of Article 32 GDPR in respect of Processor's processing of Personal Data.

4. Obligations of Processor

The Processor shall:

(a) process the Personal Data only as instructed by the Controller and on the Controller's behalf; such instruction is provided in the Services Agreement, this DPA and otherwise in documented form as

specified in clause 3 above. Such obligation to follow the Controller's instruction also applies to the transfer of the Personal Data to a Third Country or an International Organization.

(b) inform the Controller promptly if the Processor cannot comply with any instructions from the Controller for whatever reasons;

(c) ensure that persons authorized by the Processor to Process the Personal Data on behalf of the Controller have committed themselves to confidentiality or are under an appropriate obligation of confidentiality and that such persons that have access to the Personal Data Process such Personal Data in compliance with the Controller's instructions.

(d) implement the Technical and Organizational Security Measures which will meet the requirements of the Applicable Data Protection Law as further specified in the relevant Annex 4 before Processing of the Personal Data and ensure to provide sufficient guarantees to the Controller on such Technical and Organizational Security Measures.

(e) assist the Controller by appropriate Technical and Organizational Measures, insofar as this is feasible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subjects rights concerning information, access, rectification and erasure, restriction of processing, notification, data portability, objection and automated decision-making. The Processor shall maintain the Technical and Organizational Measures set forth in Annex 4 of this DPA. To the extent such feasible Technical and Organizational Measures require changes or amendments to the Technical and Organizational Measures specified in the relevant Annex 4, the Processor will advise the Controller on the costs to implement such additional or amended Technical and Organizational Measures. Once the Controller has confirmed to bear such costs, the Processor will implement such additional or amended Technical and Organizational Measures to assist the Controller to respond to Data Subject's requests.

(f) make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and in Article 28 GDPR and allow for and contribute to audits, including inspections conducted by the Controller or another auditor mandated by Controller. The Controller is aware that any in-person on-site audits may significantly disturb the Processor's business operations and may entail high expenditure in terms of cost and time. Hence, the Controller may only carry out an in-person on-site audit if the Controller reimburses the Processor for any costs and expenditures incurred by the Controller due to the business operation disturbance. Each requested audit shall meet the following requirements:

(i) no more than one audit per calendar year shall be requested or conducted and upon no less than 90 days' notice to the Processor;

(ii) shall be conducted by an internationally recognized independent auditing firm reasonably acceptable to Processor;

(iii) take place during Processor's regular business hours, pursuant to a mutually agreed upon scope of audit;

(iv) the duration of the audit must be reasonable and in any event shall not exceed two business days;

(v) no access shall be given to the data of other customers; audits will not be permitted if they interfere with Processor's ability to provide the Services to any customers;

(vi) audits shall be subject to any confidentiality or other contractual obligations of Processor or Wolters Kluwer's group (including any confidentiality obligations to other customers, vendors or other third parties);

(vii) any non-affiliated third parties participating in the audit shall execute a confidentiality agreement reasonably acceptable to Processor;

(viii) all costs and expenses of any audit shall be borne by Controller; and

(ix) any audit of a facility will be conducted as an escorted and structured walkthrough and shall be subject to Processor's security policies.

(g) notify the Controller without undue delay:

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

(ii) about any complaints and requests received directly from the Data Subjects (e.g., regarding access, rectification, erasure, restriction of processing, data portability, objection to processing of data, automated decision-making) without responding to that request, unless it has been otherwise authorized to do so;

(iii) if the Processor is required pursuant to EU or Member State law to which the Processor is subject to process the Personal Data beyond the instructions from the Controller, before carrying out such processing beyond the instruction, unless that EU or Member State law prohibits such information on important grounds of public interest; such notification shall specify the legal requirement under such EU or Member State law;

(iv) if, in the Processor's opinion, an instruction infringes the Applicable Data Protection Law; upon providing such notification, the Processor shall not be obliged to follow the instruction, unless and until the Controller has confirmed or changed it; and

(v) after the Processor becomes aware of a Personal Data Breach at the Processor. In case of such a Personal Data Breach, taking into account the nature of the processing and information available to the Processor, upon the Controller's written request, the Processor will use commercially reasonable efforts to assist the Controller with the Controller's obligation under Applicable Data Protection Law to inform the affected Data Subjects and the Supervisory Authorities, as applicable, and to document the Personal Data Breach.

(h) assist the Controller, to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor, with any Data Protection Impact Assessment as required by Article 35 GDPR that relates to the Services provided by the Processor to the Controller and the Personal Data processed by the Processor on behalf of the Controller.

(i) deal with all enquiries from the Controller relating to its Processing of the Personal Data subject to the processing (e.g., to enable the Controller to respond to complaints or requests from Data Subjects in a timely manner) and abide by the advice of the Supervisory Authority with regard to the Processing of the Personal Data transferred.

(j) that, to the extent that the Processor is required and requested to correct, erase and/or block Personal Data processed under this DPA, the Processor will do so without undue delay. If and to the extent that Personal Data cannot be erased due to statutory retention requirements, the Processor shall, in lieu of erasing the relevant Personal Data, be obliged to restrict the further Processing and/or use of Personal Data, or remove the associated identity from the Personal Data (hereinafter referred to as "blocking"). If the Processor is subject to such a blocking obligation, the

Processor shall erase the relevant Personal Data before or on the last day of the calendar year during which the retention term ends.

5. Sub-processing

(a) The Controller hereby authorizes the appointment and use of Sub-processor(s) engaged by the Processor for the provision of the Services. The Controller approves the Sub-processor(s) set out in Annex 5.

(b) The Controller acknowledges and agrees that (i) Wolters Kluwer group may be retained as Sub-processors; and (ii) the Processor and Wolters Kluwer group respectively may engage third-party Sub-processors (and permit each Sub-Processor appointed under this clause 5 to appoint sub-processors) in connection with the provision of the Services.

In case the Processor intends to engage new or additional Sub-processors, the Controller hereby provides general written authorization for the Processor to do so, provided that the Processor shall inform the Controller of any intended changes concerning the addition or replacement of any Sub-processor ("**Sub-processor Notice**") such notice to be provided on the GDPR page at https://www.cch.co.uk/softwaresupport/2015/home.asp ("**Sub-processor List Website**"). The Controller is responsible for visiting the Sub-processor List Website from time to time. If the Controller has a reasonable basis to object to the use of any such new or additional Sub-processor, the Controller shall notify the Processor promptly in writing within 14 days after receipt of the Sub-processor Notice. In the event the Controller objects to a new or additional Sub-processor, and that objection is not unreasonable, the Processor will use reasonable efforts to make available to the Controller a change in the Services or recommend a commercially reasonable change to the Controller's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new or additional Sub-processor without unreasonably burdening the Controller. If the Processor is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, the Controller may terminate (notwithstanding any contrary provision in the Services Agreement and without liability to the Controller) the affected part of the Services Agreement with respect only to those Services which cannot be provided by the Processor without the use of the objected-to new or additional Sub-processor by providing written notice to the Processor.

(c) The Processor and/or Wolters Kluwer group shall impose the same data protection obligations as set out in this DPA on any Sub-processor by contract. The contract between the Processor and the Sub-processor shall in particular provide sufficient guarantees to implement the Technical and Organizational Security Measures as specified in Annex 4, to the extent such Technical and Organizational Security Measures are relevant for the services provided by the Sub-processor. The Controller agrees that in respect of transfers of Personal Data under this DPA from the EU, the European Economic Area ("**EEA**") and/or their Member States and Switzerland to Third Countries, to the extent such transfers are subject to the Applicable Data Protection Law, the Processor shall secure the transfer under the terms of the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Decision 2010/87/EU ("**Model Clauses**") or such other mechanism approved by the European Commission and/or the UK as valid from time to time.

(d) The Processor and/or Wolters Kluwer group shall choose the Sub-processor(s) diligently.

(e) The Processor shall remain liable to the Controller for the performance of the Sub-processor's obligations, should the Sub-processor fail to fulfil its obligations. However, the Processor shall not be liable for damages and claims that ensue from the Controller's instructions to Sub-processors.

(f) The provisions of this clause 5 shall not apply to the extent Controller instructs the Processor to allow a third party to Process Controller's Personal Data pursuant to a contract that Controller has directly with the third party.

6. Limitation of liability

The liability of the Processor and/or its Affiliates, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and the Processor, whether in contract, tort or under any other theory of liability shall be exclusively governed by, the liability provisions set forth in, or otherwise applicable to, the relevant Agreement applicable to the Services. Therefore, and for the purpose of calculating liability caps and/or determining the application of other limitations on liability, any liability occurring under this DPA shall be deemed to occur under the relevant Agreement and be subject to the 'Limitation of Liability' section of the Agreement.

7. Duration and termination

(a) The terms of this DPA supplement the terms of each Agreement. The term of this DPA shall automatically expire upon the termination of the last Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the relevant Agreement.

(b) The Processor shall by the later of: (i) 90 days after the end of the provision of Services involving the processing of Personal Data; (ii) termination of the relevant Agreement; and (iii) expiration of the time period for which Personal Data is maintained pursuant to applicable disaster recovery practices for the Services, to the extent reasonably practicable, delete and procure the deletion of all copies of Personal Data processed by the Processor unless EU or Member State law requires the Processor to retain such Personal Data.

8. Miscellaneous

(a) The Processor may modify or supplement this DPA, with reasonable notice to Customer: (i) if required to do so by a Supervisory Authority or other government or regulatory entity; (ii) if necessary to comply with applicable law; (iii) to implement new or updated Model Clauses approved by the European Commission; or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 GDPR.

(b) In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this DPA shall prevail.

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

(d) This DPA and the documents referred to in it including the Agreement(s) constitute the entire understanding and agreement of the parties in relation to the processing of the Personal Data and supersede all prior agreements, discussions, negotiations, arrangements and understandings of the parties and/or their representatives in relation to such processing. Nothing in this DPA shall exclude or limit either party's liability for fraudulent misrepresentation.

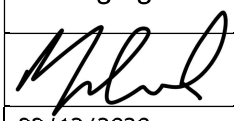
(e) This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement. Transmission of the executed signature page of a counterpart of this Agreement by email (in PDF, JPEG or other agreed format) shall take effect as delivery of an executed counterpart of this Agreement. No counterpart shall be effective until each party has executed at least one counterpart.

(f) This DPA shall be governed by English Law except to the extent that mandatory Applicable Data Protection Law applies.

(g) This DPA has been pre-signed by the Processor and shall only become legally binding upon the receipt by the Processor of a fully executed version, Customer having executed a copy of it and returned it to the Processor at data-administration@wolterskluwer.co.uk

(h) Each Party warrants it has full capacity and authority to enter into and perform its obligations under this DPA.

IN WITNESS whereof the duly authorised representatives of each party have executed this Agreement as at the Effective Date

For and On behalf of the Processor(s):	**Wolters Kluwer (UK) Limited**	**Wolters Kluwer (Ireland) Limited**
Name (written out in full):	Matthew Crook	Matthew Crook
Position:	Managing Director	Managing Director
Signature:		
Date:	09/12/2020	09/12/2020

For and On behalf of the Controller/ Please complete in full and use CAPITAL LETTERS

Name of Business (written out in full):

Company/LLP reg.no (as applicable):

Registered Business/Office Address:

Name & Position of person signing:

Signature:

Date:

The signatory confirms that he/she is fully authorised to enter into this DPA and bind the Controller to this agreement.

Products/Services Schedule

Subject to the Customer's Account and the Services Agreement at all times, as applicable:

1) Wolters Kluwer (UK) Limited

On premises products	Online products/services
CCH Central: CCH Audit Automation CCH Accounts Production / CCH ProCAP CCH Document Management CCH Personal Tax CCH Corporation Tax CCH Practice Management / CCH ProCost CCH Capital Gains and Dividend Scheduling CCH Working Paper Management CCH Fixed Asset Register CCH Central Workflow CCH Central reporting CCH Ixbrl Review & Tag CCH Trust Accounts CCH Tax Return Review CCH Partnership Tax CCH Trust Tax	-
CCH Equity	CCH Company Secretarial
CCH SecTax	Twinfield
CCH Insolvency	-

OR

2) Wolters Kluwer (Ireland) Limited

On premises products	Online products/services
CCH Personal Tax IE	-
CCH Corporation Tax IE	-
CCH Central CCH Audit Automation CCH Accounts Production CCH Document Management CCH Personal Tax CCH Corporation Tax CCH Practice Management CCH Working Paper Management CCH Fixed Asset Register CCH Central Workflow CCH Central reporting CCH Ixbrl Review & Tag	-

In respect of on premises products:

I. The Controller acknowledges and agrees it: 1) processes such categories of Personal Data and such Special Categories of Data as it wishes from time to time; 2) may transfer any such Personal Data and/or Special Categories of Data to any country subject to their own validation of the data transfer mechanisms used; 3) is responsible for implementing and maintaining its own Technical and Organizational Security Measures for the on premises products to protect the security of personal data created, collected, received, or otherwise processed by Controller which it hosts on its servers. Except at specified at II below, the Processor does NOT access and does not process any Personal Data stored on the on premises products.

II. Occasionally, at the Controller's request (and with its express permission at all times) the Processor may process such Personal Data and/or Special Categories of Data as the Controller determines and provides, transfers or permits screen sharing/ remote access to the Processor, in connection with performing obligations to provide Support Services and/or Consultancy Services from time to time. In that respect the Processor shall process such Personal Data as detailed Annexes 1-5.

Annex 1 Personal Data, purposes and description of processing operation(s)

- Personal Data and/or Special Categories of Data - all/inserted or submitted by the Controller (as applicable to the products/services in scope)
- Subject matter of processing/ description of processing operation(s): performance of Processor's obligations under the relevant Agreement and/or clause 4 (a) of this DPA

Annex 2 Processor's Contact details

Data-administration@wolterskluwer.co.uk

Annex 3 Transfers outside the EEA

Please refer to Annex 5

Annex 4 Security measures

This Annex describes the Technical and Organizational Security Measures and procedures that the Processor shall, as a minimum, maintain to protect the security of personal data created, collected, received, or otherwise obtained.

General: Technical and organizational security measures can be considered as state of the art per the conclusion of the DPA. The Processor will evaluate technical and organizational security measures over time, considering costs for implementation, nature, scope, context and purposes of processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Detailed technical measures:	Processor's position:	Modularity/ Optionality
Pseudonymization of data	X	X
Encryption of data	✓	X
Ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services	✓	X
Ability to restore the availability and access to the Personal data in a timely manner in the event of a physical or technical incident	✓	X
Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.	✓	X

✓ = Yes; X = No

Certification available: N/A

Annex 5 Sub-processor(s):

Name	Services	Location
Citrix Inc.	Facilitation of document/database transfer (Sharefile); Screen sharing/ remote access (GoToMeeting)	EEA
Wolters Kluwer	Support capability augmentation and/or DevOps	EEA; India (Model Clauses)
Salesforce.com	Support case management	EEA and/or US (Model Clauses)
Wolters Kluwer group; Microsoft	Email/correspondence; business supporting services (e.g. as above) Virtual Machine Environment for resolving support cases	EEA, India, US (Model Clauses);
Damco Solutions Ltd	Software development, consultancy and support services	India (Model Clauses)
Individual contractor(s)	During peak times and/or support escalation cases from time to time	EEA, US (Model Clauses)

Updates will be notified on the GDPR page at:
https://www.cch.co.uk/softwaresupport/2015/home.asp

In respect of Online Products

Annex 1 Personal Data, purposes and description of processing operation(s)

- Personal Data and/or Special Categories of Data - all/ within the functionality made available to the Controller (as applicable to the products/services in scope)
- Purposes of processing/ description of processing operation(s) : performance of Processor's obligations under the relevant Agreement and/or clause 4 (a) of this DPA

Annex 2 Processor's Contact details

Data-administration@wolterskluwer.co.uk

Annex 3 Transfers outside the EEA

Please refer to Annex 5

Annex 4 Security measures

This Annex describes the Technical and Organizational Security Measures and procedures that the Processor shall, as a minimum, maintain to protect the security of personal data created, collected, received, or otherwise obtained.

General: Technical and organizational security measures can be considered as state of the art per the conclusion of the DPA. The Processor will evaluate technical and organizational security measures over time, considering costs for implementation, nature, scope, context and purposes of processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Detailed technical measures:	Processor's position:	Modularity/ Optionality
Pseudonymization of data	X	X
Encryption of data	✓	X
Ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services	✓	X
Ability to restore the availability and access to the Personal data in a timely manner in the event of a physical or technical incident	✓	X

Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.	✓	X

✓ = Yes; X = No

Annex 5 Sub-processor(s)

In addition to the sub-processors at Annex 5 above

Name	Services	Location
Microsoft Azure	Hosting platform. Please see certifications at: https://www.microsoft.com/en-gb/learning/azure-certification.aspx	EEA
BottomLine Technologies	Payment processor (PCI -DSS & ISO 27001 certifications)	EEA
Twilio Inc., Sendgrid Inc., (part of Twilio)	Facilitation of SMS notifications sent by online products Facilitation of Email notifications sent by online products	US (BCR)
FCLS Group Limited	Software licence, hosting & maintenance, second line support (CCH Co Secretarial only)	EEA

Updates will be notified on the GDPR page at:
https://www.cch.co.uk/softwaresupport/2015/home.asp

Annex 6

As permitted by clause 8a) in the Data Processing Addendum ("DPA"), we are modifying and/or supplementing its terms as follows:

1. With immediate effect references in clause 5c) DPA and/or the Annexes DPA, to the EU-US Privacy Shield pursuant to Decision 2016/1250/EU as representing one of the approved mechanisms for Personal Data transfers from the EU, the European Economic Area ("EEA") to the US, shall be deleted.

2. With effect from 1st January 2021 (the "Brexit Effective Date"), and subject to the Pre-conditions at 2.1 below becoming fully satisfied on such date, the Model Clauses (as such term is defined in clause 5c) DPA) pursuant to Decision 2010/87/EU shall be deemed incorporated into and hereby supplement the DPA as between Customers of Wolters Kluwer (UK) Limited located in EU/EEA (the Data Exporter(s)) and Wolters Kluwer (UK) Limited (the Data Importer). The Data Exporters' continued use of the Data Importer's products and services under the Services Agreement, following the Brexit Effective Date will constitute the Data Exporter's acceptance of the Model Clauses which are deemed executed and part of the DPA.

2.1 Pre-conditions:

2.1.1 The UK becomes a Third Country (as such term is defined in the DPA);

2.1.2 The European Commission has not issued an adequacy decision in

respect of the UK (on the basis of its powers drawn from article 45 GDPR Transfers on the basis of an adequacy decision); and

2.1.3 There is no other authorised/ approved/agreed lawful transfer of Personal Data from the EU/EEA to the UK that takes effect/becomes applicable as a matter of law.

3. Pursuant to clause 5b) DPA, the parties further acknowledge that, in accordance with the FAQ II.1 in Article 29 Working Party Paper WP 176 "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC", the Data Exporter may provide a general consent to onward sub-processing by the Data Importer. Accordingly, the Customer provides a general consent to Wolters Kluwer (UK) Limited, pursuant to Clause 11 of the Model Clauses, to engage onward sub-processors, subject to compliance with the requirements of clause 5 DPA.

4. To the extent required, the Customer appoints Wolters Kluwer (UK) Limited as its agent for the purposes of entering into the Model Clauses with sub-processors on the Customer's behalf (in its capacity as Data Exporter) for the purpose of Processing the Personal Data based on the Services Agreement, the DPA and as otherwise instructed.

5. For the purposes of Clause 5(a) of the Model Clauses, Annexes 1 DPA shall be deemed an instruction by the Data Exporter to the Data Importer to Process Personal Data under the Services Agreement, the DPA and as otherwise instructed.

6. For the purposes of the obligations in Clause 5(d)(ii) of the Model Clauses, the Data Exporter acknowledges the Data Importer's obligations in clause 4(g)(v) DPA are applicable.

7. For the purposes of the audits described in Clauses 5(f), 11(4) and 12(2) of the Model Clauses, the Data Exporter acknowledges the provisions of clause 4(f) DPA are applicable.

8. In the case of conflict or ambiguity between the terms of any provision contained in the main body of the DPA and the Model Clause, the Model Clauses shall control.

9. Effective from the Brexit Effective Date, references in Annexes 5 DPA to Sub-processors' locations being in the EEA shall be read to mean EEA & UK.

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

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

Name of the data exporting organisation: **Wolters Kluwer (UK) Limited as agent for and on behalf of the Customer**

Address: Customer's registered office or principal business address

Tel.: +[] fax:N/A; e-mail: the email address of the primary Customer contact

Other information needed to identify the organisation: as such detail is included in the Services Agreement

(the data **exporter**)

And

Name of the data importing organisation: **Wolters Kluwer (UK) Limited**

Address: 145 London Road, Kingston upon Thames, KT26 SR

Other information needed to identify the organisation: registered in England & Wales reg no 450650

(the data **importer**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

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

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

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

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

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

Clause 2

Details of the transfer

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

---

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

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

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

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

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

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

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

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

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, 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.

in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

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

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim

against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit

of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

---

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

Clause 12

Obligation after the termination of personal data processing services

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

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

On behalf of the data importer: Wolters Kluwer (UK) Limited

Name (written out in full): Matthew Crook

Position: Managing Director

Address: 145 London Road, Kingston upn Thames, KT2 6SR

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

Signature…… 

(stamp of organisation)

On behalf of the data exporter: Wolters Kluwer (UK) Limited as agent for an on behalf of the Customer

Name (written out in full): Matthew Crook

Position: Mnaging Director

Address: c/o 145 London Road, Kingston upn Thames, KT2 6SR

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

Signature…… 

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is the Customer being (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and (ii) all Affiliates (as defined in the agreement) of Customer established within the European Economic Area (EEA); that have purchased or have access to the data importer's products and/or services under the Services Agreement.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

A provider of software solutions for tax and accounting experts who provide products and/or services to the data exporter as more fully described in the Agreement

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Personal data transferred is that of employees, workers, consultants, and clients of Data Exporter who are natural persons or as specified at Annex 1 DPA

Categories of data
The personal data transferred concern the following categories of data (please specify):

As specified at Annex 1 DPA

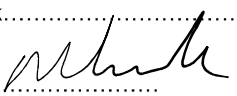
Special categories of data (if appropriate)

As specified at Annex 1 DPA

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
The purpose of processing by data importer is the performance of its obligations pursuant to the Services Agreement or as specified at Annex 1 DPA

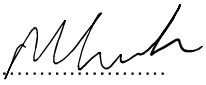
DATA EXPORTER

Name:…Matthew Crook……

Authorised Signature …

DATA IMPORTER

Name:……Matthew Crook……

Authorised Signature ………

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

As specified at Annex 4 DPA