CCH GDPR COMPLIANCE

Customer Service Terms and Conditions

Last updated 25/01/2023

By accepting this Agreement either by clicking on the "OK" button indicating e-acceptance or executing an Order Form, you (for and on behalf of the Customer), agree to these terms and conditions which are binding. If you do not agree to these terms and conditions, you must not accept this Agreement and cannot use CCH GDPR COMPLIANCE and/or any of the Services.

You agree that the Supplier may periodically update these terms and conditions (which update(s) shall be effective on the date specified). Your use of CCH GDPR COMPLIANCE following the effective date of such update(s) will constitute your acceptance of those updated terms and conditions.

Background

(A) The Supplier is in the business of providing, among other things, CCH GDPR COMPLIANCE licences which it makes available to its customers for the purpose of supporting their GDPR compliance activities.

(B) The CCH GDPR COMPLIANCE solution is made available by the Supplier to its customers under licence.

(C) The Customer wishes to use CCH GDPR COMPLIANCE in its business operations.

(D) The Supplier has agreed to provide and the Customer has agreed to take and pay for CCH GDPR COMPLIANCE strictly subject to these terms and conditions.

Agreed Terms

1. **DEFINITIONS AND INTERPRETATION**

1.1 In this Agreement, unless the context otherwise requires, the following terms have the following meanings:

"Agreement"	means the Order Form, these Customer Service Terms and Conditions, the Data Processing Addendum and any other documents expressly referenced in these;
"Authorised Users"	means those employees, agents and independent contractors of the Customer who are authorised by the Customer to access and use the Solution;
"Business Day"	means any day other than: (i) a Saturday; (ii) a Sunday; or (iii) official holidays.
"Business Hours"	means 9 am – 5.00pm on a Business Day;

"Confidential Information"	means any and all information in any form or medium obtained by or on behalf of either party from or on behalf of the other party in relation to this Agreement which is expressly marked as confidential or which a reasonable person would consider to be confidential, whether disclosed or obtained before, on or after the date of this Agreement, together with any reproductions of such information or any part of it;
"Control"	a business entity shall be deemed to "control" another business entity if it owns, directly or indirectly, in excess of 50% of the outstanding voting securities or capital stock of such business 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;
"Customer Data"	means any data inputted into the Solution by or on behalf of the Customer and/or otherwise created through use of the Solution by the Customer;
"Data Protection Legislation"	means GDPR (and/or UK GDPR, as applicable), and additional rules and implementations of EU data protection laid down in EU member state law and/or UK law including the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications) (as applicable);
"Documents"	means any customised documentation generated by the Solution following the input of Customer Data into the Solution and which is based on a Template including reports and notices;
"Effective Date"	means the commencement date noted in the Order Form;
"Fees"	means the subscription fees payable by the Customer to the Supplier for the Service as set out on the Order Form and/or otherwise notified by Supplier to the Customer and as may be amended from time to time;
"Force Majeure Event"	means any circumstance not within Supplier's reasonable control including, without limitation: (a) acts of God, flood, drought, earthquake or other natural disaster; (b)

	epidemic or pandemic; (c) terrorist attack, civil war, civil commotion or riots, war, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, or breaking off of diplomatic relations; (d) nuclear, chemical or biological contamination or sonic boom; (e) any law or any action taken by a government or public authority; (f) collapse of buildings, fire, explosion or accident; (g) any labour or trade dispute, strikes, industrial action or lockouts; and (h) interruption or failure of a utility service;
"Supplier"	means Wolters Kluwer (UK) Limited;
"GDPR"	means the European General Data Protection Regulation (EU) 2016/679;
"Intellectual Property Rights"	means any and all copyright and related rights, trade marks and service marks, trade names and domain names, rights under licences, rights in get-up, rights to goodwill or to sue for passing off, patents, rights to inventions, rights in designs, rights in computer software, database rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications (or rights to apply) for, and renewals or extensions of, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world;
"Liability"	means liability in or for breach of contract, breach of duty, torts (including negligence and intentional torts), misrepresentation, restitution or any other cause of action whatsoever relating to or arising under or in connection with this Agreement;
"Order Form"	means the Supplier's standard document which may include a quotation and which the Customer sends to the Supplier reflecting its offer to subscribe for the Services for the Fees;
"Service"	means the subscription service provided by Supplier to the Customer under this Agreement which includes use of the Solution via the Website and as more particularly described in clause 3;

"Solution"	means CCH GDPR COMPLIANCE, the SaaS solution provided by Supplier via the Website to assist organisations with GDPR compliance;
"Subscription Plan"	means a subscription plan for the Service as described on the Order Form and as may be amended from time to time by Supplier;
"Subscription Term"	means a subscription term of 12 months commencing on the Effective Date and on each subsequent anniversary;
"Template"	means a template document available within the Solution and which can be customised through the input of Customer Data to create a Document;
"Term"	means the term of the Agreement as set out in clause 2;
"Virus"	means any thing or device (including any solution, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer solution, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices;
"Website"	means the website located at www.CCHGDPR.com or such other website address as notified by Supplier from time to time.

1.2 Clause, schedule and paragraph headings shall not affect the interpretation of these Terms.

1.3 A person includes an individual, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns.

1.4 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.5 Words in the singular shall include the plural and vice versa.

1.6 A reference to one gender shall include a reference to the other genders.

1.7 A reference to a statute or statutory provision is a reference to the same as from time to time amended, extended, re-enacted or consolidated and includes any subordinate legislation for the time being in force made under it.

1.8 References to "clauses" and "Schedules" are to the clauses of, and schedules to, this Agreement; References to "Paragraphs" are to paragraphs of the relevant Schedule.

1.9 Any phrase introduced by the terms "**including**", "**include**", "**in particular**" or any similar expression, shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

1.10 A reference to "writing" or "written" includes in electronic form and similar means of communication.

2. TERM

2.1 The Agreement shall commence on the Effective Date and shall continue for the Subscription Term unless and until terminated in accordance with the terms of this Agreement.

2.2 Either party may terminate this Agreement upon providing not less than 60 days' written notice to the other party, such notice not to expire prior to the end of the then current Subscription Term.

3. SERVICE

3.1 During the Term and subject to the terms and conditions of this Agreement, the Supplier shall provide the Service.

3.2 As part of the Service, Supplier grants to the Customer a limited, non-exclusive, non-transferable and non-sub-licensable licence to access and use the Solution for its own internal business purposes.

3.3 The Customer acknowledges and accepts that the Solution may be hosted by a trusted third party hosting service provider(s) AWS in Ireland and Germany.

3.4 The Agreement only permits access to the Solution by persons who are Authorised Users. In relation to the Authorised Users, the Customer undertakes that:

3.4.1 the maximum number of Authorised Users that it authorises to access and use the Service shall not exceed the number of users permitted under the Subscription Plan subscribed to by the Customer;

3.4.2 each Authorised User shall keep a secure password for his/her use of the Service and shall keep the password secure and confidential;

3.4.3 it shall maintain a written, up to date list of current Authorised Users and provide such list to Supplier upon a written request at any time. The Customer shall notify Supplier immediately of any Authorised User that should no longer have access to the Solution and of any new Authorised User.

3.5 The Customer shall procure that Authorised Users shall not access, store, distribute or transmit via the Solution any Viruses, or any material during the course of its use of the Service that:

3.5.1 is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

3.5.2 facilitates illegal activity;

3.5.3 depicts sexually explicit images;

3.5.4 promotes unlawful violence;

3.5.5 is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

3.5.6 is otherwise illegal or causes damage or injury to any person or property;

and Supplier reserves the right, without liability or prejudice to its other rights to the Customer, to disable the Customer's access to the Solution in the event of any breach of the provisions of this clause.

3.6 The Customer shall procure that Authorised Users shall not attempt to:

3.6.1 except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties and except to the extent expressly permitted under this Agreement:

(a) copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Solution (as applicable) in any form or media or by any means; or

(b) de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Solution;

3.6.2 access all or any part of the Solution in order to build a product or service which competes with the Solution;

3.6.3 use the Solution to provide services to third parties;

3.6.4 license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Solution available to any third party except the Authorised Users;

3.6.5 attempt to obtain, or assist third parties in obtaining, access to the Solution, other than as provided under this clause 3;

3.6.6 use or knowingly permit the use of any security testing tools in order to prove, scan or attempt to penetrate the security of the Solution; and/or

3.6.7 use or launch, or knowingly permit the use or launch of, any automated system, including “robots”, “spiders” or “offline readers” that access the Solution in a manner that sends more messages to the Solution in a given period of time than a human can reasonably produce in the same period by using a conventional online web browser.

3.7 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Solution and, in the event of any such unauthorised access or use, shall promptly notify the Supplier in writing.

3.8 Access to the Solution is licensed and not sold. The Customer shall not, by virtue of this Agreement or otherwise, acquire any rights whatsoever in the Solution aside from the limited licenses granted under this Agreement. The Supplier and its licensors shall retain all right, title and interest in and to the Solution and all Intellectual Property Rights in the Solution as well as any modifications or enhancements made to the Solution.

3.9 The Customer shall comply with the Data Protection Legislation and the Data Processing Agreement ("DPA") set out in Schedule 1.

3.10 The Customer shall comply (and shall procure that the Authorised Users shall comply) with the Supplier's Acceptable Use Policy set out in Schedule 2.

4. SUPPLIER'S OBLIGATIONS

4.1 The Supplier undertakes that the Service will be provided with reasonable skill and care.

4.2 The Supplier:

4.2.1 does not warrant that the Customer's use of the Service will be uninterrupted or error-free or that the Service, Solution and/or the information obtained by the Customer through the Service, including Documents, will meet the Customer's requirements; and

4.2.2 does not warrant that the Solution, the Templates and/or any Documents comply with Data Protection Legislation. The Supplier is not a legal advisor and the Customer is solely responsible for obtaining its own legal advice as to whether the Solution, the Templates and any Documents comply with Data Protection Legislation;

4.2.3 is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Service and the Solution may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

4.2.4 shall use commercially reasonable endeavours to make the Service available 24 hours a day, seven days a week, except for planned maintenance and unscheduled maintenance.

4.3 The Supplier will, as part of the Service, provide the Customer with standard customer support services during Business Hours. Training is excluded from the Service and may be made available by the Supplier subject to additional charges and on such terms and conditions as applicable from time to time.

4.4 The Supplier confirms that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this Agreement.

4.5 The Supplier shall comply with the Data Protection Legislation and the Data Processing Agreement ("DPA") set out in Schedule 1.

5. CUSTOMER'S OBLIGATIONS

5.1 The Customer shall provide the Supplier with:

(a) all necessary co-operation in relation to this Agreement; and

(b) all information as may be reasonably required by the Supplier;

in order for the Supplier to provide the Service.

5.2 The Customer warrants that:

5.2.1 all user information including information regarding Authorised Users is accurate and that such information will be updated as necessary to maintain its completeness and accuracy;

5.2.2 comply with all applicable laws and regulations with respect to its activities under this Agreement;

5.2.3 it will ensure Authorised Users use the Service in accordance with the terms and conditions of this Agreement and the Customer shall be responsible for any Authorised User's breach of this Agreement;

5.2.4 establish adequate operational back-up systems and procedures to ensure recovery and continuity of its systems and operations in the event of a failure of the Solution;

5.2.5 ensure that its network and systems comply with the relevant specifications provided by the Supplier from time to time;

5.2.6 use current industry standard anti-malware protection solutions to reduce the risk of passing Viruses into the Solution; and

5.2.7 be solely responsible for procuring and maintaining its network connections and telecommunications links.

6. CUSTOMER DATA

6.1 The Customer shall own all right, title and interest in and to all of the Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data.

6.2 In the event of any loss or damage to Customer Data, the Customer's sole and exclusive remedy shall be for the Supplier to use reasonable commercial endeavours to restore the lost or damaged Customer Data from the latest daily back-up of such Customer Data maintained by Supplier and/or its licensors. The Supplier and/or its licensors shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party.

6.3 The Supplier shall, in providing the Service, comply with its Privacy Notice relating to the privacy and security of the Customer Data available at https://www.wolterskluwer.com/en-gb/solutions/software-tax-accounting/privacy-notice as such document may be amended from time to time by the Supplier in its sole discretion.

7. FEES AND PAYMENT

7.1 The Customer shall pay the Fees to the Supplier in accordance with this clause 7 and without any deduction, discount, counterclaim, set-off or withholding.

7.2 The Customer shall provide to the Supplier valid, up-to-date and complete contact and billing details.

7.3 The Supplier shall invoice the Customer annually in advance for the Fees. Invoice shall be payable within 30 days from the date of invoice.

7.4 If the Supplier has not received payment of any sums due under this Agreement by the due date, and without prejudice to any other rights and remedies it may have, the Supplier:

7.4.1 may, without liability to the Customer, suspend the Service and disable the Customer's and all Authorised User's access to all or part of the Solution and the Supplier shall be under no obligation to provide any or all of the Service to the Customer while the invoice(s) concerned remain unpaid; and

7.4.2 charge interest which shall accrue on a daily basis on such due amounts at an annual rate equal to 4% over the then current base lending rate of Supplier's bankers in the UK from time to time, commencing on the due date and continuing until fully paid, whether before or after judgment.

7.5 All amounts and fees stated or referred to in this Agreement:

7.5.1 shall be payable in pounds sterling;

7.5.2 are non-cancellable and non-refundable;

7.5.3 are exclusive of value added tax, which shall be added to the invoice(s) at the appropriate rate.

7.6 The Supplier shall be entitled to review and increase the Fees on expiry of the first Subscription Term and annually thereafter upon not less than 60 days' prior notice to the Customer.

7.7 The Customer agrees to reimburse the Supplier for any reasonable costs that the Supplier incurs when recovering any amount owed by the Customer, including debt collection agency costs and reasonable legal costs.

8. INTELLECTUAL PROPERTY RIGHTS

8.1 The Customer acknowledges and agrees that Supplier and/or its licensors own all Intellectual Property Rights in the Solution and the Templates.

8.2 The Supplier confirms that it has all the rights in relation to the Solution and the Templates that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of this Agreement.

9. CONFIDENTIALITY

9.1 Each party may be given access to Confidential Information from the other party in order to perform its obligations under this Agreement. A party's Confidential Information shall not be deemed to include information that:

9.1.1 is or becomes publicly known other than through any act or omission of the receiving party;

9.1.2 was in the other party's lawful possession before the disclosure;

9.1.3 is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or

9.1.4 is independently developed by the receiving party, which independent development can be shown by written evidence.

9.2 Subject to clause 9.4 each party shall hold the other's Confidential Information in confidence and not make the other's Confidential Information available to any third party (save that the Supplier shall be permitted to make a disclosure within the Supplier's group, to its officers, directors, professional advisors and (sub)contractors) or use the other's Confidential Information for any purpose other than the implementation of this Agreement.

9.3 Each party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of this Agreement.

9.4 A party may disclose Confidential Information to the extent such Confidential Information is required to be disclosed by law, by any governmental or other regulatory authority or by a court or other authority of competent jurisdiction, provided that, to the extent it is legally permitted to do so, it gives the other party as much notice of such disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this clause 9.4, it takes into account the reasonable requests of the other party in relation to the content of such disclosure.

9.5 Neither party shall be responsible for any loss, destruction, alteration or disclosure of Confidential Information caused by any third party.

9.6 The Supplier acknowledges that the Customer Data is the Confidential Information of the Customer.

9.7 The above provisions of this clause 9 shall survive termination of this Agreement (for a period of 3 years), however arising.

10. INDEMNITY

10.1 The Supplier shall defend the Customer, its officers, directors and employees against any claim that the Solution infringes any Intellectual Property Rights ("Claim") and shall indemnify the Customer for any amounts finally awarded against the Customer in judgment or settlement of such Claims, provided that:

10.1.1 Supplier is given prompt written notice of any such Claim;

10.1.2 the Customer provides reasonable co-operation to Supplier and/or its licensors in the defence and settlement of such Claim; and

10.1.3 the Supplier and/its licensors are given sole authority to defend or settle the Claim.

10.2 In the defence or settlement of any claim, the Supplier and/or its licensors may at their sole discretion, procure the right for the Customer to continue using the Solution, replace or modify the Solution so that it becomes non-infringing or, if such remedies are not reasonably available, terminate this Agreement without any additional liability or obligation to pay damages or other additional costs to the Customer.

10.3 In no event shall the Supplier, its employees, agents, sub-contractors and/or its licensors be liable to the Customer including under clause 10.1, to the extent that the Claim is based on:

10.3.1 a modification of the Solution by anyone other than the Supplier and/or its licensors;

10.3.2 the Customer's use of the Solution in breach of this Agreement; and/or

10.3.3 the Customer's use of the Solution after notice of the alleged or actual infringement from the Supplier and/or its licensors or any appropriate authority.

10.4 This clause 10 sets out the Customer's sole and exclusive rights and remedies, and the Supplier's (including Supplier's employees', agents' and sub-contractors' and/or its licensors') entire obligations and liability, for any Claim.

11. LIMITATION OF LIABILITY

11.1 Nothing in this Agreement excludes or limits the Liability of the Supplier:

11.1.1 for fraud or fraudulent misrepresentation;

11.1.2 for death or personal injury caused by the Supplier's negligence;

11.1.3 which it cannot exclude or limit as a matter of applicable law.

11.2 Except as expressly and specifically provided in this Agreement:

11.2.1 all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this Agreement; and

11.2.2 the Service is provided to the Customer on an "As Is" basis.

11.3 Subject to clause 11.1:

11.3.1 The Supplier shall have no Liability for any loss of profits, loss of business, depletion of goodwill and/or similar losses; loss or corruption of data or information; pure economic loss; non-pecuniary loss; third party loss; and/or any special, indirect or consequential loss, costs, damages, charges or expenses; in all cases however arising under this Agreement and whether direct or indirect, foreseeable or otherwise; and

11.3.2 the total aggregate Liability of the Supplier arising out of or in connection with this Agreement (unless otherwise excluded or limited) shall be limited to the total Fees paid by the Customer to the Supplier during the 12 months immediately preceding the date of the event giving rise to the Liability.

11.4 The exclusions and limitations of Liability under clause 11.3 have effect in relation to both any Liability expressly provided for under this Agreement and to any Liability arising by reason of the invalidity or unenforceability of any term of this Agreement.

11.5 The Supplier shall have no Liability unless the Customer shall have served notice in writing of any facts which may give rise to Liability (and were not excluded by this Agreement) within 2 (two) years of the date the Customer either became aware of the circumstances giving rise to Liability or the date the Customer ought reasonably to have become so aware.

11.6 The Customer acknowledges and agrees that the limitations on or exclusions of Liability are fair and reasonable having regard to the commercial relationship between the parties.

12. TERMINATION

12.1 Without affecting any other right or remedy available to it, either party may terminate this Agreement with immediate effect by giving written notice to the other party if:

12.1.1 the other party is in material breach of any of its obligations under this Agreement, and, where such material breach is capable of remedy, the other party fails to remedy such breach within a period of 30 days of being notified of such breach by the party; and/or

12.1.2 the other party gives notice to any of its creditors that it has suspended or is about to suspend payment; or if it shall be unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986; or an order is made or a resolution is passed for the winding-up of the other party or an administration order is made or an administrator is appointed to manage the affairs, business and property of the other party or a receiver and/or manager or administrative receiver is appointed in respect of all or any of the other party's assets or undertaking; or circumstances arise which entitle the court or a creditor to appoint a receiver and/or manager or administrative receiver or administrator or which entitle the court to make a winding-up or bankruptcy order; or the other party takes or suffers any similar or analogous action to any of these events in this clause 12.1.2 in any jurisdiction.

12.2 Termination of this Agreement shall be without prejudice to any accrued rights or remedies of either party.

12.3 Termination of this Agreement shall not affect the coming into force, or continuance in force, of any provision which is expressly or by implication intended to come into or continue in force on or after such termination.

12.4 The Supplier reserves the right without notice and without Liability to the Customer, to terminate any Services in the event that its licensors suffer a change of Control event, or become involved in any capacity in any business concern which, in Supplier's reasonable opinion, competes with the business of the Supplier (or that of its group).

12.5 On termination of this Agreement for any reason:

12.5.1 the licence granted under this Agreement shall immediately terminate and the Supplier shall be entitled to disable Customer's use of the Solution;

12.5.2 the Supplier may destroy or otherwise dispose of any of the Customer Data in its possession 3 months after termination; and

12.5.3 any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination shall not be affected or prejudiced.

13. FORCE MAJEURE

13.1 If Supplier is subject to a Force Majeure Event, it shall not be in breach of this Agreement and shall be excused from performance under this Agreement while and to the extent it is unable to perform due to any Force Majeure Event.

13.2 If the circumstance of a Force Majeure Event continues for a period of 60 days or longer, either party shall have the right to terminate this Agreement upon written notice to the other.

14. WAIVER

14.1 A waiver of any right or remedy under this Agreement is only effective if given in writing and shall not be deemed a waiver of any subsequent breach or default. No failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it preclude or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

15. SEVERANCE

15.1 If any provision (or part of a provision) of this Agreement is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions shall remain in force.

15.2 If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

16. NON-SOLICITATION

16.1 In order to protect the Supplier's legitimate business interests and each of its group companies, the Customer covenant with the Supplier, for itself and as agent for each of the Customer's group companies (if any) that the Customer shall not (and shall procure that no member of the Customer's group shall) (except with the Supplier's prior written consent):

16.1.1 attempt to solicit or entice away; or

16.1.2 solicit or entice away;

from the Supplier's employment or service (or any of the Supplier's group companies) the services of any Restricted Person (as that term is defined in clause 16.2) other than by means of a national advertising campaign open to all-comers and not specifically targeted at Supplier's staff or any of it group companies.

16.2 For the purposes of clause 16.1, a Restricted Person shall mean any firm, company or person employed or engaged by Supplier or any of Supplier's group companies during the Subscription Term who has been engaged in the provision of services or the management of this Agreement either as principal, agent, employee, independent contractor or in any other form of employment or engagement.

17. ENTIRE AGREEMENT

17.1 This Agreement and any documents referred to in it, constitute the whole agreement between the parties and supersede any previous arrangement, understanding or agreement between them relating to the subject matter of this Agreement.

17.2 Each of the parties acknowledges and agrees that in entering into this Agreement it does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this Agreement or not) relating to the subject matter of this Agreement, other than as expressly set out in this Agreement.

17.3 Neither party excludes or limits its liability for fraud or fraudulent misrepresentation.

18. ASSIGNMENT

18.1 The Customer may not assign, sub-licence, novate or transfer any right, benefit or interest and/or any of its obligations under this Agreement, without the Supplier's prior written consent.

18.2 The Supplier shall be entitled to assign, sub-licence, novate or transfer any right, benefit or interest and/or any of its obligations under this Agreement.

19. NO PARTNERSHIP

19.1 Nothing in this Agreement is intended to or shall operate to create a partnership between the parties, or authorise either party to act as agent for the other, and neither party shall

have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power).

20. THIRD PARTY RIGHTS

20.1 This Agreement does not confer any rights on any person or party (other than the Parties and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999.

21. NOTICES

21.1 Any notice required to be given under this Agreement shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post or email to the other party at such address as may have been notified by that party for such purposes.

21.2 A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in Business Hours, at 9 am on the first Business Day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post. A notice sent by email to the email address set out above shall be deemed to have been received on the day it is sent if that is a Business Day or otherwise on the next Business Day.

22. VARIATION

22.1 The Supplier may periodically update this Agreement (which update(s) shall be effective on the date specified) and will advise the Customer by email or through other means of notification reasonably available. The Customer's continued use of the Service following the effective date of such update(s) will constitute the Customer's acceptance of those updated terms and conditions.

23. GOVERNING LAW AND JURISDICTION

23.1 This Agreement and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) are governed by, and construed in accordance with, the laws of England.

23.2 The parties submit to the exclusive jurisdiction of the English courts except that the Supplier:

23.2.1 has the right to sue in any jurisdiction in which the Customer is operating or has assets; and

23.2.2 and/or its licensors, have the right to sue for breach of Intellectual Property Rights in any country where they believe that infringement or a breach of this Agreement relating to Intellectual Property Rights might be taking place.

Schedule 1

Data Processing Addendum

These terms are supplemental to the CCH GDPR Compliance – Customer Service Terms and Conditions, and are entered between the Customer ("the **Controlle**r") and Wolters Kluwer (UK) Ltd, 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 ("the **Processor**").

Hereinafter jointly also to be referred to as the "**Parties**" and each separately as a "**Party**".

WHEREAS, the Controller and the Processors are party to the Agreement concerning the provision of the Service (as such term is defined in CCH GDPR Compliance – Customer Service Terms and Conditions) by the Processor to the Controller. A short summary is included in Annex 1.

The Processor may periodically update this DPA (which update(s) shall be effective on the date specified).In each case the Processor shall advise the Controller by email or through notification on CCH GDPR Compliance or at https://www.wolterskluwer.com/en-gb/solutions/software-tax-accounting/terms-conditions. Controller's continued use of the Service following the effective date of such update(s) will constitute its acceptance of those updated terms and conditions.

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 Agreement ("**DPA**") with effect from 25 /01/2023 or the Effective Date (if later) 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;
"Applicable/Data Protection Law"	shall mean from 25 May 2018 onwards, the General Data Protection Regulation (EU) 2016/679 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 the Controller and the Processor, and additional rules and implementations of EU data protection laid down in European member state law or UK law;

"Controller"	shall mean the Customer, who determines as a natural or legal person alone or jointly with others the purposes and means of the Processing of Personal Data;
"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 into effect from 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;
"Services Agreement"	shall mean the Agreement concluded between the Controller and the Processor setting out the terms and conditions for the provision of the Service;
"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;
“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 Service;
"Supervisory Authority"	shall mean an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR and/or the UK Information Commissioner’s Office (“ICO”);
"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 or the ICO has not decided that the country, a territory or one or more specified sectors within that country, ensures an adequate level of protection;
“UK GDPR”	shall mean the retained EU law version of the GDPR, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018) and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419); 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 Wolters Kluwer (UK) Limited 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 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 obtained 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 and/or UK 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 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 to the extent such feasible Technical and Organizational Measures require changes or amendments to the Technical and Organizational Measures specified in 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/or UK 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 Processor 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 or UK 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 or UK law prohibits such information on important grounds of public interest; such notification shall specify the legal requirement under such EU or Member State law or UK 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 and/or UK 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.

(c) 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 though CCH GDPR Compliance or at https://www.wolterskluwer.com/en-gb/solutions/software-tax-accounting/terms-conditions (**"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.

(d) 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 UK, EU, the European Economic Area ("EEA") and/or their Member States 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:

(i) the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Decision 2010/87/EU ("Model Clauses");
(ii) where GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs");
(iii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and/or
(iv) or such other mechanism approved by the European Commission and/or the ICO and valid from time to time.

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

(f) 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.

(g) 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, 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 Services Agreement applicable to the Service. 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 Services Agreement and be subject to the 'Limitation of Liability' section of the Services Agreement.

7. Duration and termination

(a) The term of this DPA is identical with the term of the Services Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Services 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 Services 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 UK, 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 the applicable Supervisory Authority; or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 GDPR (or UK 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 shall be governed by English Law except to the extent that mandatory Applicable Data Protection Law applies.

(e) This DPA and the documents referred to in it including the Services Agreement 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.

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

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

- Personal Data – all/inserted or submitted by the Controller (as applicable to the Service in scope) namely: Contact details such as name, addresses, telephone numbers, email addresses; user activity and user preferences; device details; browser history details; location details, electronic identification data including IP addresses and information collected through cookies; login details, contractual details including services provided.
- Special Categories of Data - none
- Subject matter of processing/ description of processing operation(s) : performance of Processor's obligations under the Services 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 UK, EU/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-processors

Name	Services	Location
Compliance Technology Solutions BV	Supplier's licensor	EEA & UK
Salesforce.com	Support case management	EEA & UK and/or US (EU SCCs, UK SCCs)
Wolters Kluwer group; Microsoft	Email/correspondence; Virtual Machine Environment for resolving support cases	EEA & UK US (EU SCCs, UK SCCs)
Individual contractor(s)	During peak times and/or support escalation cases from time to time	EEA & UK

Schedule 2

Acceptable Use Policy

Last updated: 22/05/2018

Your use of CCH GDPR Compliance is subject to this Acceptable Use Policy. By using CCH GDPR Compliance, you will be deemed to have accepted and agreed to be bound by this Acceptable Use Policy. We may make changes to the Acceptable Use Policy from time to time. We will notify you of such changes by any reasonable means, including by posting the revised version of the Acceptable Use Policy on CCH GDPR Compliance. You can determine when we last changed the Acceptable Use Policy by referring to the 'LAST UPDATED' statement above. Your use of CCH GDPR Compliance following changes to the Acceptable Use Policy will constitute your acceptance of those changes. If you do not agree to the Acceptable Use Policy, please refrain from using CCH GDPR Compliance.

1 You shall not access, store, distribute or transmit any Viruses, or any documentation or other material during the course of its use of the Services that:

1.1 is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

1.2 facilitates illegal activity;

1.3 depicts sexually explicit images;

1.4 promotes unlawful violence;

1.5 is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

1.6 is otherwise illegal or causes damage or injury to any person or property;

and shall procure that no Authorised User shall undertake such activity through access to the CCH GDPR Compliance. We reserve the right, without notice or liability to you, to disable your access to the Service or to any material that breaches the provisions of this Acceptable Use Policy.

2 You shall not, and shall procure that each of your Authorised Users shall not:

2.1 except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties:

2.1.1 attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of CCH GDPR Compliance and/or documentation (as applicable) in any form or media or by any means; or

2.1.2 attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the CCH GDPR Compliance; or

2.1.3 access all or any part of the Service and documentation in order to build a product or service which competes with the Service and/or the documentation; or

2.1.4 use the Service and/or documentation to provide services to third parties save as permitted by the relevant agreement; or

2.1.5 license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services and/or Documentation available to any third party except the Authorised Users, or

2.1.6 attempt to obtain, or assist third parties in obtaining, access to the Service and/or documentation without our express permission.

2.2 You shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Service and/or the documentation and, in the event of any such unauthorised access or use, promptly notify us.

3 You shall not, and shall not cause or permit others to:

3.1 perform or disclose any benchmarking, scalability, availability or performance testing of the Service; or

3.2 perform or disclose vulnerability scanning, network reconnaissance, port and service identification or penetration testing of the Services.

4 We do not apply a fixed limit to the amount of data you may store using CCH GDPR Compliance; however this does not give you the right to store an unlimited amount of data. In the event your data exceeds the average amount of data stored in CCH GDPR Compliance by other authorised users, by more than 50%, we shall inform you that your data storage has reached maximum

capacity. If you do not then reduce or cause the reduction of your data, we shall be entitled to charge a reasonable increase in the applicable fees. In the event you do not agree with the increased fees, we shall have the right to terminate your access to the Service without penalty by giving you 30 days written notice.