DATA PROTECTION ANNEX

Effective: July 15, 2022

In accordance with the "Data Protection" section of the Agreement from which this Annex is linked, this Data Protection Annex (**"Annex"**) applies to and is incorporated into the Agreement to the extent that CCH Processes any Personal Data about Data Subjects located in the EEA or the UK when performing its obligations under the Agreement.

1. Definitions. Capitalized terms used but not defined in this Annex will have the same meanings as set forth in the Agreement. In this Annex, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

"**Agreement**"	means the Terms of Use for CCH Online Content Services together with the applicable Customer Agreement agreed to between CCH Incorporated and the Customer and from which this Annex is linked;
"**CCH Personal Data**"	means any and all Personal Data about you and Data Subjects working for you that is obtained by CCH as part of the administration and performance of its obligations under the Agreement, including without limitation, Your Personal Data;
"**Data Protection Laws**"	means the EU GDPR and the UK GDPR and laws implementing, replacing or supplementing these laws when applicable;
"**EEA**"	means the European Economic Area;
"**EU**"	means the European Union;
"**EU GDPR**"	means the EU General Data Protection Regulation 2016/679 and any applicable national laws made under it;
"**Restricted Transfer**"	means a transfer of Your Personal Data from CCH and/or to a subprocessor where such transfer would be prohibited by Data Protection Laws in the absence of appropriate safeguards required for such transfers under Data Protection Laws.
"**Retained EU Law**"	means as defined in the European Union (Withdrawal) Act 2018;
"**UK**"	Means the United Kingdom;
"**UK GDPR**"	means the UK Data Protection Act 2018 ("DPA 18") and the EU GDPR as it forms part of Retained EU Law and includes all subordinate legislation and relevant regulations;
"**Your Personal Data**"	means any Personal Data about Data Subjects located in the EEA or UK that is Processed by CCH as part of the use of the Online Services under the Agreement and is provided to CCH by you when you use the Online Services.

The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing", "Processor" and "Supervisory Authority" shall have the meanings ascribed to them in applicable Data Protection Laws, and their cognate terms shall be construed accordingly.

Where there is a reference to a specific article or provision of the EU GDPR such reference shall be taken to include (and extend to) any equivalent provision or obligation set out in the UK GDPR as applicable.

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

2. ROLES AND SCOPE.

2.1 Your Personal Data. For the purposes of this Annex, to the extent the Online Services are used to Process Your Personal Data, CCH is a separate Controller of Your Personal Data Processed by it.

2.2 CCH Personal Data. For the purposes of this Annex, CCH is a separate Controller of CCH Personal Data Processed by it.

2.3 International Transfers. You acknowledge that CCH is located in the United States of America and that CCH may process CCH Personal Data, including Your Personal Data, at a destination outside the EEA or UK and that such CCH Personal Data and Your Personal Data may be processed by CCH personnel or a Processor of CCH operating outside the EEA or UK in countries that the European Commission (or in relation to the UK, the UK Government) has not yet decided offer adequate data protection in accordance with Data Protection Law ("Third Countries"). You further acknowledge and agree that:

(a) If the processing (including storage) of Your Personal Data involves a Restricted Transfer from the EEA and/or Switzerland to a jurisdiction outside of the EEA or Switzerland, as applicable, the parties agree that such transfer(s) will be carried out in accordance with and subject to the 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 annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (“EU SCCs”). Where You are acting as a controller of Your Personal Data, the parties agree to comply with Module 1 of the EU SCCs set forth in the Appendix 3 to this Annex. To the extent there is any conflict between this Annex and the EU SCCs, the terms of the EU SCCs will prevail.

(b) If the processing (including storage) of Your Personal Data involves a Restricted Transfer from the UK, the parties agree that such transfer(s) will be carried out in accordance with and subject to the International Data Transfer Agreement A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (“UK IDTA”) as set out in Appendix 4. To the extent there is any conflict between this Addendum and the UK IDTA, the terms of the UK IDTA will prevail.

2.4 Assistance. You agree that you shall provide all information and documents reasonably requested of you by CCH or CCH's representative(s) to allow CCH to satisfy its obligations under this Annex and Data Protection Laws relating to Your Personal Data and CCH Personal Data.

3. PROCESSING OF YOUR PERSONAL DATA

3.1 Your responsibilities. You shall have sole responsibility for ensuring Your Personal Data is Processed in accordance with the applicable Data Protection Laws, including:

(a) ensuring that Your Personal Data is Processed lawfully, fairly and in a transparent manner in relation to the Data Subjects, including by ensuring that all necessary fair processing information has been provided in writing to, and all necessary consents obtained from, the Data Subjects in relation to the Processing of such Personal Data by the parties and by third parties on their behalf.

(b) ensuring that Your Personal Data is collected for specified, explicit and legitimate purposes based on a legal grounds for Processing as may be required from time to time by applicable Data Protection Laws and not further processed in a manner that is incompatible with those purposes.

3.2 CCH's responsibilities.

(a) CCH shall in determining the extent to which Your Personal Data is required in relation to the purposes for which Your Personal Data is to be Processed by CCH, only request Your Personal Data that is relevant, adequate and not excessive in accordance with Data Protection Laws. CCH shall have sole responsibility for using reasonable efforts to ensure that Your Personal Data, at the time it is first made available to you through the Online Services, accurately reflects the data that you provided to CCH. At all times thereafter, you shall be solely responsible for ensuring that Your Personal Data remains accurate and up-to-date in accordance with Data Protection Laws.

(b) CCH shall maintain the security practices and policies for the protection of Your Personal Data as set forth in Appendix 2. You warrant that You have assessed the security measures set out in Appendix 2 and has determined that they satisfy the requirements of Data Protection Laws in respect of CCH's processing of Your Personal Data.

(c) As required under Data Protection Laws, CCH shall inform You without undue delay after it becomes aware of any Personal Data Breach of Your Personal Data that was in its possession or control, providing a description of the nature of the breach and the information referred to in Article 33(b)-(d) of the EU GDPR as soon as it becomes available. In addition, each party shall consult in good faith with the other and provide the other with assistance, information and cooperation in the investigation, notification, mitigation and remediation of each such Personal Data Breach. While CCH may take any information provided by you into account, only CCH shall determine the content of any related public statements and any required notices to the affected Data Subjects and/or the relevant Supervisory Authorities in connection with a Personal Data Breach involving Your Personal Data in its possession.

3.3 Each party's responsibilities. Each party shall:

(a) ensure that Your Personal Data that is in its possession or control is kept for no longer than is necessary for the purposes for which Your Personal Data are processed in accordance with Data Protection Laws.

(b) in relation to Your Personal Data that is in its possession or control, be responsible for ensuring that Your Personal Data is Processed in a manner designed to ensure appropriate security of Your Personal Data including protection against Personal Data Breaches as required by Data Protection Laws.

Except to the extent that this Section 3 (Processing of Your Personal Data) allocates responsibility for compliance with particular provisions of Data Protection Laws to a particular party, each party shall comply with its respective obligations under Data Protection Laws in relation to Your Personal Data.

4. PROCESSING OF CCH PERSONAL DATA

4.1 Use of CCH Personal Data. CCH may process CCH Personal Data for the following purposes:

(a) perform under and manage and make decisions about the Agreement and any matters (such as making the Online Services available to Customer's users, customer support, invoicing and fee arrangements) arising in connection with the Agreement;

(b) communicate with you and the Data Subjects that work for you in relation to matters arising under or in connection with the Agreement and in connection with services and products that CCH may offer from time to time;

(c) comply with regulatory and legal obligations to which CCH is subject;

(d) establish, exercise and defend legal rights and claims;

(e) manage customer relationships;

(f) manage risk, perform quality reviews and manage security and operations;

(g) record, monitor, assess and analyze the use of the Online Services, and improve the content and the functionality of the Online Services,

(h) market, advertise and send reports to you or Customer;

(i) compile statistical and other information related to the performance, operation and use of the Online Services, including for the purposes of sending reports to you or Customer, and

(j) CCH's internal financial accounting, information technology and other administrative support services,

(collectively, "**Processing Purposes**"). You will ensure that there is no prohibition or restriction in relation to CCH's use thereof that would prevent or restrict CCH from Processing the CCH Personal Data for the Processing Purposes. You shall also ensure that all consents have been obtained and all notices have been issued, as necessary under the Data Protection Laws, to enable the CCH Personal Data to be disclosed to and used by CCH for the Processing Purposes as a separate Controller.

4.2 Additional Information Regarding Processing. Appendix 1 to this Annex sets out certain information regarding the processing of CCH Personal Data. The parties may amend Appendix 1 from time to time as the parties may reasonably consider necessary. Nothing in Appendix 1 (including as amended pursuant to this Section 4.1) confers any right or imposes any obligation on any party to this Annex.

5. GENERAL TERMS.

5.1 Governing law and Jurisdiction. Except to the extent set out otherwise in the Appendix 3 and Appendix 4, and as necessary to comply with Data Protection Laws, the parties to this Annex hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Annex, including disputes regarding its existence, validity or termination or the consequences of its nullity and this Annex and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

5.2 Severance; Order of Precedence. Should any provision of this Annex be invalid or unenforceable, then the remainder of this Annex shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. In the event of a conflict or discrepancy between (a) this Annex and any term of the Agreement, this Annex shall take precedence with respect to such conflict, (b) the EU SCCs and the provisions of this Annex, the EU SCCs shall prevail, and (c) this Annex and the UK IDTA, the UK IDTA shall prevail.

Appendix 1 to Data Protection Annex

DETAILS OF PROCESSING OF PERSONAL INFORMATION

Categories of data subjects whose personal data is transferred

Customer's users of the Online Services, including Customer's professional resources (such as lawyers or accountants) which may include Customer's employees, independent contractors and partners, performing research tasks on behalf of Customer.

Categories of personal data transferred

First and last names of natural persons
Business contact information, such as email addresses and telephone numbers
Login name and password
Usage data and search terms

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Use of the Online Services doesn't anticipate the transfer of special categories of data.

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

Continuous basis as necessary for the purposes of the transfer detailed below.

Nature of the processing

See the description of the purposes below.

Purpose(s) of the data transfer and further processing

The transfer is made for the following purposes:

(i) perform under and manage and make decisions about this Agreement and any matters (such as making the Online Services available to Customer's users, customer support, invoicing and fee arrangements) arising in connection with this Agreement,

(ii) communicate with you and your users that work for you in relation to matters arising under or in connection with this Agreement and in connection with services and products that CCH may offer from time to time,

(iii) comply with regulatory and legal obligations to which CCH is subject,

(iv) establish, exercise, and defend legal rights and claims,

(v) manage customer relationships,

(vi) manage risk, perform quality reviews, and manage security and operations,

(vii) record, monitor, assess and analyze the use of the Online Services and improve the content and the functionality of the Online Services,

(viii) market, advertise and send reports to you or Customer,

(ix) compile statistical and other information related to the performance, operation and use of the Online Services, including for the purposes of sending reports to you or Customer, and

(x) internal financial accounting, information technology and other administrative support services.

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

Personal data may be processed to the extent necessary for the performance of data importer's obligations (including during the period of subscription and any renewal), and for the time necessary to achieve the purposes for which the personal data is collected, in accordance with the data importer's data retention and disaster recovery practices and the applicable Data Protection Laws. When the data importer no longer needs personal information, the data importer takes all reasonable steps to remove it from its systems and records or take steps to properly anonymize it.

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

(i) Service providers or subprocessors who perform certain functions on data importer's behalf, such as to provide analytics and site usage information, implementation and onboarding, provide outsourced help with the operations of the electronic content platforms, provide marketing and promotional assistance, and provide other services related to the operation of data importer's business.

(ii) Marketing partners and vendors to develop, deliver and report on targeted advertising of our services and products either online or in emails sent by data importer, or data importer's marketing partners, to data exporter.

(iii) Public and government authorities or other legal entities for purposes of, among things, (a) to comply with or as required by applicable law, including laws outside data exporter's country of residence, (b) to comply with legal process, either within or outside data exporter's country of residence, (c) to respond to requests from public and government authorities, including public and government authorities outside data exporter's country of residence, for national security and/or law enforcement purposes, (d) to enforce data importer's terms and conditions, and (e) to allow data importer to pursue available remedies or limit the damages that it may sustain.

(iv) Affiliates of data importer who support data importer products and services and with whom data importer shares certain back-office functions.

(v) Customers with respect to the data relating to its users.

Appendix 2 to Data Protection Annex

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

INFORMATION SECURITY

CCH Online Content Offerings
Wolters Kluwer Global Information Security Program
June 2022

CCH Incorporated is a Wolters Kluwer company. This document helps customers and product users understand the policies, frameworks, and controls in place to maintain the enterprise security of Wolters Kluwer information systems, information, assets, environments, and customer information. Based on the type of information being stored in specific products, the products may have additional more stringent policies, controls, and frameworks in place. CCH, through its Tax & Accounting and Legal & Regulatory divisions, offers a broad range of content products through a variety of digital platforms to address the research needs of tax, accounting, legal and compliance professionals. The functionality of each of our digital research platforms is not intended to be used to store, capture, or transmit customer client confidential or personally identifiable information. Except with respect to IP authentication or some single sign-on authentication methods that may be offered with specific platforms, only limited personal information (first name, last name, business email and password) is collected from customers/users for purposes of authentication and use of platform functionality such as saving search results so that one might return to a research task at a later time.

1. Security Program. Wolters Kluwer maintains a written global information security program of policies, procedures and controls aligned to recognized industry standards, governing the processing, storage, transmission and security of data (the "Security Program"). The Security Program mandates industry-standard practices designed to protect data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed. Wolters Kluwer updates the Security Program to address (i) new and evolving security threats, (ii) changes to industry standards, (iii) technological advances in security tools, and (iv) amendments required following risk assessments undertaken pursuant to 1.3 below. Additionally, all security policies and standards governing the Security Program are reviewed, updated, and approved annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.

2. Security Organization. Wolters Kluwer has implemented a three-tiered information security management structure to facilitate the management, architecture, and operations of security functions. The Security Council oversees the management of this structure. Members of the Security Council include leadership representatives including commercial division CTOs, Legal, Internal Audit, Internal Controls, the Global Information Security team, and Risk Management. Wolters Kluwer has a Chief Information Security Officer who is responsible for oversight, management, and monitoring of Wolters Kluwer's Security Program.

3. Audits. Annually, the Wolters Kluwer Security Program is audited by an independent third party. For select systems, applications and services, Wolters Kluwer receives third party audits for compliance with SOC 2 Type 2.

4. Facilities. Offices and data center facilities that are owned or leased by Wolters Kluwer include physical access restrictions and fire detection and fire suppression systems both localized and throughout the buildings.

5. Personnel Security. Users who are given access to Assets must abide by the Wolters Kluwer Acceptable Use Policy. Wolters Kluwer performs background screening on employees and all contractors who have access to Wolters Kluwer information and customers' information, subject to applicable laws and regulations.

6. Endpoint Security. Wolters Kluwer implements and maintains security mechanisms on endpoints, including firewalls, automated locking of devices after a specified period of inactivity, updated anti-virus, an advanced endpoint detection and response (EDR) solution, and full disk encryption. Wolters Kluwer restricts personnel from disabling security mechanisms.

7. Training and Awareness. Wolters Kluwer maintains a security and privacy awareness program that includes both regularly scheduled and unannounced training and education of its personnel, including any contractors or other third parties working on its behalf with access to data or Assets.

8. Vendor Risk Management. Wolters Kluwer maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Wolters Kluwer information and customers' information for appropriate security and privacy controls and business disciplines. Before Wolters Kluwer provides a vendor with access to personal information or any other sensitive information of Wolters Kluwer employees or customers, or critical Assets, it is required that appropriate security controls are in place. Access by vendors is required to be limited to only the access required to provide the contracted-for services. Security controls are required to be implemented to ensure that vendor access is limited appropriately. Periodic reviews of vendors, including third-party security audits, may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures.

9. Separation of Environments. For Wolters Kluwer critical Assets, Wolters Kluwer deploys separate development, QA, and production environments. Wolters Kluwer does not use customer data in development and maintains controls to prevent such use.

10. Encryption. Wolter Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data. Encryption keys are created and protected with at least the same level of security and access control as the data being protected. The encryption strength is based on industry standards for strong encryption and does commensurate with the data classification.

11. Firewall System. Industry standard firewalls are installed and managed to protect Wolters Kluwer systems by monitoring all entry connections routed to the Wolters Kluwer environment.

12. Data Backup. Wolters Kluwer maintains a backup plan to ensure all critical data is backed up without affecting system operations. The type and frequency of backup and type of backup media used takes into consideration the volume of data, criticality of data and recovery time constraints.

13. Business Continuity. Wolters Kluwer maintains business continuity plans ("BCP") which include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein.

14. Disaster Recovery. Wolters Kluwer (i) maintains an IT disaster recovery plan ("DR"); (ii) tests the DR plan at least once every year; (iii) makes available summary test results which will include the actual recovery point and recovery times; and (iv) documents any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the services from being recovered in accordance with the DR plan.

15. Incidents and Events Management. Wolters Kluwer has a cross-functional global information security incident response team that provides 24/7, 365 days a year proactive security monitoring, management, and response, in accordance with Wolters Kluwer's established corporate incident management plan. Wolters Kluwer's security team will promptly analyze potential security incidents and events to assess the impact, determine if immediate risk exists, and take immediate action to mitigate such damage.

Appendix 3 to Data Protection Annex

MODULE 1 CONTROLLER TO CONTROLLER

STANDARD CONTRACTUAL CLAUSES

The parties hereby agree that they will comply with the EU Standard Contractual Clauses: Module 1, which are incorporated herein by reference, a copy of which can be found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en. The Parties agree that the following terms apply:

1. **Clause 7:** The Parties have chosen not to include Clause 7.

2. **Clause 11(a):** The Parties do not incorporate the optional language allowing a data subject to lodge a complaint with an independent dispute resolution body at no cost to the data subject.

3. **Clause 13(a):** Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

4. **Clause 17:** These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

5. **Clause 18(b):** The Parties agree that those shall be the courts of the Netherlands.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The subscribing Customer (as defined in the Agreement) to the Online Services (or an affiliate of such Customer, if applicable)

- Contact details: data exporter can be contacted through the contract details set forth in the Customer Agreement (as defined in the Agreement).
- Activities relevant to the data transferred under these Clauses: entering into the Customer Agreement and utilizing the Online Services being subscribed to for its internal business purposes.
- Signature and date: as reflected in the Customer Agreement.
- Role: controller

Data importer(s): CCH Incorporated

- Contact details:
  - 2700 Lake Cook Road, Riverwoods Illinois 60015 United States of America
  - Phone 800-234-1660 for Legal & Regulatory and 800-344-3734 for Tax and Accounting
  - For the Tax and Accounting division of data importer – TAAPrivacySecurity@wolterskluwer.com
  - For the Legal & Regulatory division of data importer – LRUSPrivacy@wolterskluwer.com
- Activities relevant to the data transferred under these Clauses: entering into the Customer Agreement and authenticating users onto the Online Services being subscribed to and performance under the Agreement.
- Signature and date: as reflected in the Customer Agreement.
- Role: controller

B. DESCRIPTION OF TRANSFER

See Appendix 1.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority for purposes of this Annex I.C shall be the supervisory authority in the Member State in which the data exporter or the data exporter's Article 27 representative, as applicable, is located. In the event that the data exporter is not located in a Member State and does not have an Article 27 representative, the competent supervisory authority shall be the Dutch Data Protection Authority.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITYOF THE DATA

Refer to Appendix 2.

AMENDMENTS TO ENABLE THE TRANSFER OF DATA FROM SWITZERLAND TO A THIRD COUNTRY

Pursuant to the FDPIC's guidance titled "The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts," dated 27 August 2021, the parties are adopting the GDPR standard for all data transfers under the FADP and under the GDPR. To the extent Personal Information is transferred outside of Switzerland to a country with an inadequate level of data protection, the following amendments to the Standard Contractual Clauses provided for in this Appendix 3 shall apply:

1. Annex I.C: The competent supervisory authority shall be the FDPIC, insofar as the data transfer is governed by the FADP; and shall be the EU authority referenced in Annex I.C insofar as the data transfer is governed by the GDPR.
2. The term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
3. The Standard Contractual Clauses shall also protect the data of legal entities until the entry into force of the revised FADP.

APPENDIX 4
UK INTERNATIONAL DATA TRANSFER AGREEMENT (UK IDTA)

Part 1: Tables

Table 1: Parties and signatures

Start date	The Effective Date of the Annex	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Refer to Customer Agreement	Refer to Customer Agreement
Key Contact	Refer to Customer Agreement	Refer to Customer Agreement
Importer Data Subject Contact	Refer to Customer Agreement	Refer to Customer Agreement
Signatures confirming each Party agrees to be bound by this UK IDTA	Refer to Customer Agreement	Refer to Customer Agreement

Table 2: Transfer Details

UK country's law that governs the UK IDTA:	The jurisdiction in which the Data Exporter is located.
Primary place for legal claims to be made by the Parties	The jurisdiction in which the Data Exporter is located.
The status of the Exporter	In relation to the Processing of the Transferred Data the Exporter is a Processor or Sub-Processor insofar as it is processing data on behalf of another entity. If Exporter is not processing data on behalf of another entity, Exporter is a Controller.
The status of the Importer	In relation to the Processing of the Transferred Data, Importer is a Controller.
Whether UK GDPR applies to the Importer	UK GDPR may apply to the Importer's Processing of the Transferred Data
"Term"	The Importer may Process the Transferred Data for no longer than is

	necessary for the Purpose.
Ending the UK IDTA before the end of the Term	The Parties cannot end the UK IDTA before the end of the Term unless there is a breach of the UK IDTA or the Parties agree in writing.
Ending the IDTA when the Approved IDTA changes	Which Parties may end the UK IDTA as set out in Section 29.2: Exporter
Can the Importer make further transfers of the Transferred Data?	The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	There are no specific restrictions.
Review Dates	First review date: Effective Date of the Agreement The Parties must review the Security Requirements at least once each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment, to the extent that Importer is made aware of such changes; Importer will conduct a review at the time of contract renewal

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of that data outlined in Appendix 1 of the Annex. The categories of Transferred Data will update automatically if the information is updated in the Agreement or Annex.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to that data outlined in Appendix 1 of the Annex. The categories of special category and criminal records data will update automatically if the information is updated in the Agreement or Annex.
Relevant Data Subjects	The Data Subjects of the Transferred Data are those data subjects outlined in Appendix 1 of the Addendum. The categories of Data Subjects will update automatically if the information is

	updated in the Agreement or Annex.
Purpose	The Importer may Process the Transferred Data for the purposes set out in the Annex. The purposes will update automatically if the information is updated in the Agreement or Annex.

Table 4: Security Requirements

See Appendix 2 of the Annex. The Security Requirements will update automatically if the information is updated in the Agreement or Annex.

Part 2: Extra Protection Clauses

N/A

Part 3: Commercial Clauses

N/A

Part 4: Mandatory Clauses

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved UK IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.