LEGISWAY DATA PROCESSING ADDENDUM

This Legisway Data Processing Addendum (this "**Addendum**") is effective as of December 1, 2022 ("**Addendum Effective Date**") and forms a part of the Legisway Service Terms and Conditions (the "**Terms and Conditions**") between CCH Incorporated, a Wolters Kluwer company ("**CCH**") and an individual, institution or organization ("**Customer**") subscribing to the Product pursuant to an order form or agreement (together with the Terms and Condition, and as may be amended from time to time, the "**Agreement**"). In the course of providing the Services (as defined below), CCH may process personal data (as defined below) on behalf of Customer, and CCH agrees to comply with the following provisions with respect to any such personal data.

1. Definitions. Capitalized terms used but not defined in this Addendum will have the same meanings as set forth in the Agreement. In this Addendum, the following terms shall have the meaning set out below:

a. "**Affiliate**" has the meaning given to such term in the Agreement.

b. "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., as amended or superseded from time to time (including the California Privacy Rights Act of 2020), and regulations promulgated thereunder.

c. "**Customer Personal Data**" means any personal data of a data subject that is processed by CCH on behalf of Customer to perform the Services under the Agreement.

d. "**control**" (or variants of it) means the ability, whether directly or indirectly, to direct the management and action of an entity by means of ownership, contract or otherwise.

e. "**Data Protection Laws**" means the EU GDPR, the UK GDPR and the CCPA and laws implementing, replacing or supplementing these laws where applicable.

f. "**EU GDPR**" means the EU General Data Protection Regulation 2016/679.

g. "**Restricted Transfer**" means a transfer of Customer 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.

h. "**Retained EU Law**" means as defined in the European Union (Withdrawal) Act 2018.

i. "**Services**" means the Legisway Services, as well as all related services (such as Support services), provided to Customer by CCH pursuant to the Agreement.

j. "**Subprocessor**" means any party (including CCH's Affiliates and any other third parties) appointed by CCH to process Customer Personal Data to perform the Services.

k. "**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.

l. The terms "**controller**", "**data subject**", "**personal data**", "**personal data breach**", "**processor**", "**processing**", and "**supervisory authority**" shall have the meanings ascribed to them in applicable Data Protection Laws, and their cognate terms shall be construed

accordingly. In the event of a conflict between the aforementioned terms under Data Protection Laws, the definition which confers the highest level of protection to the data that is the subject of this Addendum shall apply.

m. 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.

2. Customer Warranties. Customer warrants that:

a. Customer's processing of the Customer Personal Data is based on legal grounds for processing as may be required by Data Protection Laws and it has made and shall maintain throughout the term of the Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by Data Protection Laws with respect to CCH's processing of Customer Personal Data under this Addendum and the Agreement; and

b. It is entitled to and has all necessary rights, permissions and consents to transfer the Customer Personal Data to CCH and otherwise permit CCH to process the Customer Personal Data on its behalf, so that CCH may lawfully use, process and transfer the Customer Personal Data in order to carry out the Services and perform CCH's other rights and obligations under this Addendum and the Agreement.

3. Controller and Processor. For purposes of this Addendum, Customer is the controller of the Customer Personal Data and CCH is the processor of such data, except when Customer acts as a processor of Customer Personal Data, in which case CCH is a subprocessor. Customer and its Affiliates, as their respective controllers, shall determine the purposes of collecting and processing Customer Personal Data.

4. Scope of Processing.

a. In order for CCH to provide the Services under the Agreement, CCH will process Customer Personal Data. Appendix 1 to this Addendum sets out certain information regarding the processing of Customer 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(a)) confers any right or imposes any obligation on any party to this Addendum.

b. CCH shall only process Customer Personal Data (i) in accordance with the documented instructions described in this Addendum, and (ii) for the purposes of fulfilling its obligations under the Agreement. In processing Customer Personal Data, CCH will (i) comply with its obligations under all Data Protection Laws, and (ii) notify Customer in accordance with applicable Data Protection Laws if CCH determines it can no longer meet its obligations under Data Protection Laws or this Addendum. If any Data Protection Laws to which CCH is subject requires CCH to process Customer Personal Data in a manner contrary to Customer's instructions, CCH shall inform Customer in advance of any relevant processing of the affected Customer Personal Data, unless the relevant Data Protection Laws prohibits this on important grounds of public interest.

c. CCH shall inform Customer if, in CCH's opinion, an instruction given by Customer under this Section 4 infringes EU Law. CCH shall have the right to suspend processing of

Customer Personal Data until Customer's instruction is clarified to the extent that it no longer infringes Data Protection Laws.

d. CCH shall not (i)"sell" or "share" (as those terms are defined by the CCPA) Customer Personal Data; (ii) combine Customer Personal Data with personal data CCH receives from or on behalf of another person or entity or collects from its own interactions with a data subject unless permitted by Data Protection Laws; (iii) retain, use, or disclose Customer Personal Data for any purpose other than for the business purposes specified in the Agreement, including retaining, using, or disclosing it for a commercial purpose other than the business purposes specified in the Agreement or as otherwise permitted under Data Protection Laws; or (iv) retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and CCH. To the extent required by Data Protection Laws, CCH certifies that it understands these restrictions and will comply with them.

e. Customer reserves the right to take reasonable and appropriate steps to help ensure that CCH processes Customer Personal Data in a manner consistent with Customer's obligations under Data Protection Laws, including without limitation the right, upon notice, to stop and remediate any unauthorized processing of Customer Personal Data.

5. Confidentiality. CCH shall ensure that each of its personnel that is authorized to process Customer Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Security.

a. CCH shall, in relation to Customer Personal Data, (a) implement and maintain reasonable and appropriate technical and organizational safeguards designed to protect Customer Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure and will ensure that all such safeguards comply with Data Protection Laws, and (b) on reasonable request at Customer's cost, assist Customer in ensuring compliance with Customer's obligations pursuant to Data Protection Laws, taking into account the nature of the processing and the information available to CCH.

b. CCH shall maintain the security practices and policies for the protection of Customer Personal Data as set forth in Appendix 2. Customer warrants that it has 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 Customer Personal Data.

7. Subprocessors. Customer hereby authorizes CCH to appoint Subprocessors in accordance with this Section 7, subject to any restrictions in the Agreement. CCH will bind Subprocessors with written agreements that require them to provide at least the level of data protection required of CCH by this Addendum relative to the Subprocessor's activities relating to the Services. Customer authorizes CCH's engagement of CCH's Affiliates, and the third party(ies) listed in Appendix 1, as Subprocessors. In case CCH intends to engage new or additional Subprocessors, CCH will inform Customer in writing (which may be by email or other Product-enabled notification to Customer's Product Administrator) of such additions or replacements (the "**Subprocessor Notice**"). If Customer has reasonable grounds proving that significant risks for the protection of its Customer Personal Data exist with such new or additional Subprocessor(s), Customer will notify CCH in writing within 30 days of the date of the Subprocessor Notice, detailing the basis for the objection. CCH will work with Customer in good faith to make available a commercially reasonable change in the provision of the

Services or recommend a commercially reasonable change to such Customer's configuration or use of the Services to avoid processing of Customer Personal Data by the objected-to new or additional Subprocessor(s) without unreasonably burdening Customer, in either case which avoids the use of the Subprocessor(s). Where such a change cannot be made within 90 days from CCH's receipt of Customer's objection notice, notwithstanding anything in the Agreement, Customer, may, as its sole remedy, by written notice to CCH with immediate effect terminate that portion of the Agreement that relates to the Services that require the use of such new or additional Processor. CCH shall be responsible for the acts and omissions of any Subprocessors as it is to Customer for its own acts and omissions in relation to the matters provided in this Addendum. The provisions of this Section 7 shall not apply to the extent Customer instructs CCH to allow a third party to Process Customer Personal Data pursuant to a contract that Customer has directly with the third party.

8. Data Subject Requests. To the extent legally permitted, CCH will promptly notify Customer if CCH or any Subprocessor receives any complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to Data Protection Laws) related to Customer Personal Data. Taking into account the nature of the processing, CCH shall assist Customer at Customer's cost and request, by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfillment of Customer's obligation to respond to requests for exercising such data subjects' rights.

9. Data Breach. CCH shall notify Customer without undue delay once CCH becomes aware of a personal data breach affecting Customer Personal Data. CCH shall, taking into account the nature of the processing and the information available to CCH, use commercially reasonable efforts to provide Customer with sufficient information, including to the extent known a detailed description of the personal data breach, the type of data that was the subject of the personal data breach, the identity of the affected data subjects, the steps CCH has taken or intends to take in order to mitigate and remediate such personal data breach, and any other information as required by Data Protection Laws.

10. Data Protection Impact Assessments. CCH shall, taking into account the nature of the processing and the information available to CCH, provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for Customer to fulfill its obligations under Data Protection Laws.

11. Destruction of Customer Personal Data.

a. Subject to Section 11.b. below, or as otherwise required by applicable law, CCH will promptly and in any event by the later of: (i) 90 days after the date of cessation of any Services involving the processing of Customer Personal Data; (ii) termination of the Agreement, and (iii) expiration of the time period for which Customer 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 Customer Personal Data processed by CCH. For the avoidance of doubt, CCH may retain Customer Personal Data as required by Data Protection Laws.

b. For so long as CCH and each Subprocessor retains Customer Personal Data in accordance with this Section 11, CCH's obligations of confidentiality with respect to such Customer Personal Data will continue and CCH will ensure that such Customer Personal Data is only processed as necessary and for no other purpose.

12. Audit.

a. Subject to Sections 12(b) and (c), CCH shall make available to Customer upon reasonable written request, information that is reasonably necessary to demonstrate CCH's compliance with this Addendum. Customer shall be responsible for any costs and expenses of CCH arising from the provision of such information and audit rights.

b. Customer's information and audit rights only arise under Section 12(a) above to the extent that the Agreement and/or any other information available to Customer in relation to the Services does not otherwise give Customer information and audit rights meeting the requirements of Section 12(a) above.

c. Customer is aware that any in-person on-site audits are likely to significantly disturb CCH's business operations, including operations relating to the Services being provided pursuant to the Agreement. Customer shall ensure that its auditors make reasonable efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to CCH's premises, equipment, personnel and business while its auditor personnel are on those premises in the course of such an audit or inspection. 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 CCH;

   ii. shall be conducted by an internationally recognized independent auditing firm reasonably acceptable to CCH;

   iii. take place during CCH'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 CCH's ability to provide the Services to any customers;

   vi. audits shall be subject to any confidentiality or other contractual obligations of CCH or CCH's Affiliates (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 CCH;

   viii. all costs and expenses of any audit shall be borne by Customer; and

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

d. CCH shall immediately inform Customer if, in CCH's opinion, an instruction in relation to Customer's rights under this Section 12 infringes Data Protection Laws. CCH shall have the right to suspend processing of Customer Personal Data until Customer's instruction is clarified to the extent that it no longer infringes Data Protection Laws.

13. Data Transfer.

a. If the processing (including storage) of Customer Personal Data involves a Restricted Transfer from the European Economic Area ("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 Customer is acting as a controller of Customer Personal Data, the parties agree to comply with Module 2 of the EU SCCs as set out in Appendix 3. To the extent there is any conflict between this Addendum and the EU SCCs, the terms of the EU SCCs will prevail.

b. If the processing (including storage) of Customer Personal Data involves a Restricted Transfer from the United Kingdom ("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.

14. Miscellaneous.

a. Except as otherwise set forth herein, all terms and conditions of the Agreement will continue in full force and effect as set forth therein and amended thereby. Nothing in this Addendum reduces CCH's obligations under the Agreement in relation to the protection of Customer Personal Data or permits CCH to process (or permit the processing of) Customer Personal Data in a manner that is prohibited by the Agreement.

b. Notwithstanding any terms of the Agreement to the contrary, in the event and to the extent of any conflict between the terms and conditions of (i) this Addendum and applicable law, the provision(s) of the applicable law shall govern; (ii) this Addendum and the EU Standard Contractual Clauses, the provision(s) of the EU Standard Contractual Clauses shall prevail; (iii) this Addendum and the UK IDTA, the UK IDTA shall prevail; and (iv) this Addendum and the Agreement, the provision(s) that are more protective of Customer Personal Data shall govern. CCH shall comply with the terms of this Addendum during the term of the Agreement and during any period during which CCH may have access to Customer Personal Data.

c. CCH may modify or supplement this Addendum, 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 EU Standard Contractual Clauses or UK IDTA, as applicable, approved by the European Commission or UK government, as applicable; or

iv. To adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the EU GDPR.

d. Without prejudice (i) the Standard Contractual Clauses or UK IDTA, as applicable; or (ii) as otherwise necessary to comply with Data Protection Laws this Addendum will be governed by the laws of the country or territory stipulated in the Agreement.

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

APPENDIX 1

DETAILS OF PROCESSING OF PERSONAL DATA

This Appendix includes certain details of the processing of Personal Data:

Subject matter and duration of the processing of Personal Data

This Addendum addresses the processing of Customer Personal Data in connection with Customer's subscription to, and CCH's hosting and provision of, the Legisway online service (a software-as-a service application) pursuant to the terms of the Agreement. Legisway is an information and document repository of organization legal information, such as that relating to key contracts, other documents, policies, claims, legal entities and intellectual property and other organization information. CCH will process the Customer Personal Data during the term of the Agreement (including any renewal) and until the later of: (i) 90 days after the date of cessation of any Services involving the processing of Customer Personal Data, (ii) the expiration of any continuing obligations of CCH to retain Customer Personal Data under the Agreement, and (iii) the expiration of the time period for which Customer Personal Data is maintained pursuant to applicable disaster recovery practices for the Services.

The nature and purpose of the processing of Personal Data

CCH will process Customer Personal Data as necessary to perform the Services and fulfill Customer's subscription to the Legisway Service, as further instructed by Customer, and including:

- For the operation, maintenance and development of the Legisway Service,
- To perform Services and fulfill Customer's subscription to the Legisway Service, as further instructed by Customer
- For providing Services related to the inherent functionality of the Legisway Service,
- For hosting the Product,
- For implementation services,
- For Support, and
- For providing Services relating to the availability of the Customer Personal Data (such as disaster recovery purposes).

The types of Personal Data to be processed

Customer may input Customer Personal Data into the Legisway Service or otherwise provide Customer Personal Data in connection with its subscription to the Legisway Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include in its standard configuration, the following basic categories of Personal Data:

- First and last names of natural persons
- Titles
- Contact information (including home and work street and email addresses, telephone numbers, IP address)
- Marital status
- Citizenship information
- Governmental identification information, including drivers' license information, passport information

- Professional life data
- Related person's data

The categories of data subject to whom the Personal Data relates

Customer may input Customer Personal Data into the Legisway Service or otherwise provide Customer Personal Data in connection with its subscription to the Legisway Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include information with respect to the following categories of data subjects: employees, independent contractors, officers, directors, advisors, parties and counter-parties to contracts, claimants, and vendors.

List of current Subprocessors:

- Amazon Web Services (hosting provider, United States of America)
- DELLA AI Ltd. (contract review analytics and support services, England)
- Microsoft Corporation (Azure)(hosting provider, DELLA AI, United States of America)
- MongoDB, Inc. (Atlas) (server management, DELLA AI, United States)
- Elasticsearch, Inc. (server management, DELLA AI, United States)
- Wolters Kluwer N.V. affiliates, including Wolters Kluwer Italia (support and development), Wolters Kluwer Technology B.V. (Digital eXperience Group, development and support relating thereto, Netherlands), Wolters Kluwer Global Business Services B.V. (hosting, support related thereto, Netherlands)

APPENDIX 2

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

INFORMATION SECURITY

CCH currently maintains the security practices with respect to its Legisway software as a service product that are described in this Annex II. CCH is also a Wolters Kluwer company and as such is subject to and abides by the Wolters Kluwer Global Information Security Program which is described further in the attachment to this Annex II. Notwithstanding any provision to the contrary, CCH/Wolters Kluwer may update or change these security practices from time to time at its discretion however the overall level of security measures will not be materially diminished without notifying Legisway customers. The U.S. instance of Legisway is currently hosted on Amazon Elastic Compute Cloud (Amazon EC2) (https://aws.amazon.com/it/ec2/details/).

The Legisway service security program is designed to (i) maintain the availability of the Legisway services and its systems and customer information, (ii) control access to the Legisway services and its systems and customer information, and (iii) maintain the confidentiality and integrity of customer information within the Legisway service. Mechanisms of the information security program include the governance risk and compliance teams within IT-Security, risk management, including vendor risk review, logging and monitoring, internal and external audits/assessments, internal controls assessment, internal and external penetration and vulnerability assessments, contract management, security awareness, security consulting and policy exception reviews. More specifically, the Legisway service security program is comprised of the following:

1. Policies and Risk Assessment. CCH has implemented an Information Security Policy that encompasses a variety of policies for managing information and technology assets intended to protect underlying applications and data. Policies are reviewed on a periodic basis. Information security risk assessments are also conducted on a periodic basis.

2. Human Resources. U.S. based Legisway employees undergo background checks and participate in security awareness training on a regular basis.

3. Legisway Infrastructure & Role Separation. Resources that support infrastructure and application services are delineated access privileges based on job responsibilities limiting access privileges to that necessary to perform responsibilities. Infrastructure credentialing requires management approval and business processes are implemented to periodically review level of privileges and address changes in role, privilege revocation and termination. CCH implements minimum standard password policy addressing complexity, age and history of password controls.

4. Customer Credential Management. Application credentials are managed by customers.

5. Data Protection. Customer data is encrypted in transit and at rest on production servers. Unique data keys are generated for each customer. Customer data is backed up daily and backups are kept for 30 days. Data is destroyed using secured techniques.

6. Environment Separation. Legisway maintains physical and/or logical environment separation for the Legisway.com application, including separate development, testing, staging and production environments. The production application is hosted on Amazon Elastic Compute Cloud (Amazon EC2), https://aws.amazon.com/it/ec2/details/, which includes access controls,

onsite security, fire suppression, uninterruptable power supply, backup generators, redundant pathways, components, power and cooling systems.

7. Availability. The computing components are deployed with one or more redundant backups in a high available environment configuration (in separate data centers), which includes a disaster recovery environment. Health and performance monitoring is conducted on all computing systems. Capacity planning is periodically assessed.

8. Operations Management. CCH maintains release management, change management, incident management and security management processes. CCH tracks key performance metrics.

9. Vulnerability and Penetration Testing. CCH conducts internal and external vulnerability and penetration testing of the Legisway application and infrastructure on a periodic basis.

APPENDIX 3

MODULE 2: CONTROLLER TO PROCESSOR

STANDARD CONTRACTUAL CLAUSES

The parties hereby agree that they will comply with the EU Standard Contractual Clauses: Module 2, 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 9(a):** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

3. **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.

4. **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.

5. **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.

6. **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 Legisway Service Terms and Conditions) to the Legisway online service (or an affiliate of such Customer, if applicable).

- Contact details: data exporter can be contacted through the contact details set forth in the Order Document (as defined in the Legisway Service Terms and Conditions).
- Activities relevant to the data transferred under these Clauses: entering into the Order Document and utilizing the Legisway online services for its internal business purposes
- Signature and date: as reflected in the Order Document
- Role: controller

Data importer(s): CCH Incorporated

- Contact details:

  2700 Lake Cook Road, Riverwoods Illinois 60015 United States of America

  Phone: 1-800-234-1660 (within the U.S.) or +1-301-678-7100 (outside of the U.S.)

  Email: customer.service@wolterskluwer.com (customer support)

  wklrus-privacy@wolterskluwer.com (privacy)

- Activities relevant to the data transferred under these Clauses: entering into the Order Document and fulfilling Customer's subscription to the Legisway online services
- Signature and date: as reflected in the Order Document
- Role: processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer may input Customer Personal Data into the Legisway online service or otherwise provide Customer Personal Data in connection with its subscription to the Legisway online service, the extent of which is determined and controlled by Customer in its sole discretion but which may include information with respect to the following categories of data subjects: employees, independent contractors, officers, directors, advisors, parties and counter-parties to contracts, claimants, and vendors.

Categories of personal data transferred

Customer may input Customer Personal Data into the Legisway online service or otherwise provide Customer Personal Data in connection with its subscription to the Legisway online service, the extent of which is determined and controlled by Customer in its sole discretion, but which may include in its standard configuration, the following basic fields that can be filled in by Customer:

- First and last names of natural persons
- Titles

- Contact information (including home and work street, email addresses, telephone numbers, IP address)
- Marital status
- Citizenship information
- Governmental identification information, including drivers' license information, passport information
- Professional life data
- Related person's data

As Data Controller, Customer can add other personal data with the "additional fields" function.

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 Legisway online service 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 continuous basis).

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

Nature of the processing

See description of the purposes below.

Purpose(s) of the data transfer and further processing

The data exporter, or an affiliate of data exporter, may transfer personal data to the data importer which will then process the personal data transferred for the following processing activities:

- For the operation, maintenance, and development of the Legisway online service
- To perform services and fullfil Customer's subscription to the Legisway online service, as further instructed by Customer
- For providing services related to the inherent functionality of the Legisway online service
- For hosting the Product
- For implementation services
- For Support
- For providing Services relating to the availability of the Customer Personal Data (such as disaster recovery purposes)

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

Subscribing Customer Personal Data may be processed during the time term agreed to with the subscribing Customer (including the period of subscription and any renewal) and until the later of: (i) 90 days after the date of cessation of any Services involving the processing of Customer Personal Data, (ii) the expiration of any continuing obligations of CCH to retain Customer Personal Data under the Agreement, and (iii) the expiration of the time period for which Customer Personal Data is maintained pursuant to applicable disaster recovery practices for the Legisway online services.

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

Transfers may be made to service providers or processors who perform certain functions on data importer's behalf, such as hosting of the Legisway online service and other services related to the operation of the data importer's business. Transfers may also be made to affiliates of data importer who support the data importer's products.

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 Customer or the Customer's Article 27 representative, as applicable, is located. In the event that Customer 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 Addendum	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Refer to Order Document	Refer to Order Document
Key Contact	Refer to Order Document	Refer to Order Document
Importer Data Subject Contact	Refer to Order Document	Refer to Order Document
Signatures confirming each Party agrees to be bound by this UK IDTA	Refer to Order Document	Refer to Order Document

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 the Exporter's Processor or Sub-Processor.
Whether UK GDPR applies to the Importer	UK GDPR applies to the Importer's Processing of the Transferred Data

"Linked Agreement"	The agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data is the Agreement and this Addendum.
"Term"	The Importer may Process the Transferred Data for the period for which the Linked Agreement is in force.
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: 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	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1to the authorised receivers (or the categories of authorised receivers) set out in Appendix 1 or otherwise approved in accordance with Section 7 (Subprocessors) of the Addendum.
Review Dates	First review date: Effective Date of the Addendum 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 Addendum. The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement.
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 Addendum. The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement.

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

Table 4: Security Requirements

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

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.