

Data Processing Addendum



In the course of providing the Software Services and Professional Services to Customer pursuant to the Agreement ("Services"), Provider may process Personal Data on behalf of Customer. This Data Processing Addendum ("DPA") and its schedule "Description of Personal Data Processing" which is incorporated into this DPA, are subject to and made part of the Agreement and complement the provisions of the Schedule "General Terms and Conditions" as regards the rights and obligations of the Parties relating to the Processing of Personal Data by Provider pursuant to article 28 of the GDPR.

1. Definitions

Capitalized terms used in this DPA have the meaning set forth in the Main Body or in the applicable Schedule. Additional terms in this DPA are defined as follows:

Applicable Data Protection Law shall mean, as applicable to each Party respectively, the national laws and regulations implementing the GDPR and the GDPR itself;

Controller: shall mean the natural or legal person alone, or jointly with others, who determines the purposes and means of the Processing of Personal Data;

Data Breach: shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored, or otherwise Processed;

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;

Data Subject: shall mean an identifiable person who can be identified, directly or indirectly, particularly 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;

EEA: shall mean the European Economic Area;

EU Standard Contractual Clauses (or EU SCCs): shall mean the Annex to the "Commission Implementing Decisions (EU) 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 C/2021/3972", or any subsequent version thereof, published by the European Commission (which will automatically apply). References to a "Module" refers to the applicable Module within the EU SCCs,

International Organization: shall mean an organization and its subordinate bodies governed by public international law or any other body 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);

Process(ed/es)/ Processing: shall mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor: shall mean the Party who Processes Personal Data on behalf of Controller under this DPA;

Sub-processor: shall mean any party engaged by Processor to process Personal Data to perform certain Services under the Agreement;

Supervisory Authority: shall mean an independent public authority established by a Member State pursuant to Article 51 of the GDPR;

Technical and Organizational Security Measures: shall mean those appropriate measures aimed at protecting Personal Data against Data Breaches to ensure a level of security appropriate to the risk;

Third Country: shall mean a country outside the EEA

2. Scope

For the purpose of this DPA, Provider is the Processor of Personal Data and Customer is the Controller of the Personal Data. The purpose of this DPA is to define, according to article 28 of the GDPR, the conditions under which Processor is entitled, on behalf of Controller who has mandated Processor by virtue of the Agreement, to carry out the Personal Data Processing operations defined in the Agreement as necessary to provide the Services under the Agreement.

Customer is Provider's single point of contact: if other controllers have rights against Provider, Customer exercises these rights on their behalf and warrants that it obtained all necessary authorizations from them. Provider is released from its obligations, including its information and notification obligations towards another controller than Customer once Provider has fulfilled its obligations to Customer.

The Processing operations (categories of Personal Data, type of Data Subject, etc.) and the Technical and Organizational Security Measures in relation to the Services provided under the Agreement are described in the Schedule "Description of Personal Data Processing" available at <https://www.wolterskluwer.com/de-de/solutions/legal-software/legal-terms-conditions>, which may be updated as the Software Services evolve, and the updated terms are applicable as of the date of availability of the new version of the Software Services.

3. CUSTOMER'S OBLIGATIONS

3.1 As Controller, Customer will ensure that any Personal Data provided to Processor by, or on behalf of, Customer has been collected lawfully, fairly and in a transparent manner to enable such Personal Data to be processed by Provider. In particular, Customer is solely responsible for the lawfulness of the Processing and must identify the legal basis for Processing.

3.2 Customer must provide Provider documented instructions relating to the Processing. Said instructions are contained in the Agreement, this DPA and the Description of Personal Data

Processing Schedule. Customer may provide additional reasonable instructions to Provider. If the execution of an additional instruction requires the implementation of Technical and Organizational Security Measures customized for Customer that are not necessary according to the Applicable Data Protection Law that applies to Provider and this results in additional costs, Provider shall inform Customer of these costs. Provider will comply with the instructions only after receiving written confirmation from Customer that Customer shall pay such additional costs. Customer's instructions will be provided in writing (email possible) unless in the event of an emergency or other specific circumstance requiring spoken communication. Any unwritten instructions must be confirmed as soon as possible in writing by Customer and in any event no later than twenty-four (24) hours after the unwritten instructions have been given. In addition, when Customer is not located in the country where Provider has its registered office, Customer shall inform Provider about specific obligations that apply to Provider under mandatory local laws applicable to Customer in order for the Parties to determine the appropriate actions.

3.3 Customer must provide information to the Data Subjects about the Processing operations. Customer is responsible for responding to Data Subjects' requests to exercise their rights. If it is not possible for Customer to obtain directly the information and data necessary for the processing of a Data Subject's request to exercise their rights, Customer will request any necessary information and data to Provider, who will assist, as far as possible, Customer in fulfilling the obligation to comply with the requests to exercise the rights of the Data Subject.

4. PROVIDER'S OBLIGATIONS

4.1 Unless obliged to do so by the law of the European Union or the law of a Member State, Provider will Process the Personal Data on behalf of Customer only in accordance with the documented instructions of Controller. This obligation to comply with Customer's instructions is also applicable for the transmission of Personal Data to a Third Country or International Organization.

Provider shall immediately inform Customer if, in its opinion, an instruction constitutes a violation of the Applicable Data Protection Law. In such a case, Provider may suspend the provision of the Services under the Agreement and will not be required to follow the instruction in question until Customer's instruction is clarified to the extent that it no longer violates the Applicable Data Protection Law. Provider will also inform Customer if Provider is not, for any reason whatsoever, able to comply with an instruction from Customer.

4.2 Provider shall ensure that persons authorized by Provider to Process the Personal Data on behalf of Customer are bound to confidentiality or are under an appropriate legal obligation of confidentiality and that such persons that have access to the Personal Data Process such Personal Data in compliance with Customer's instructions. In addition, if a Sub-processor Processes Customer Data, provisions of Section 5 below shall apply.

4.3 Provider shall implement the Technical and Organizational Security Measures within the scope of responsibility of Provider taking into account the nature, scope, context and purposes of the Processing, the state of the art and the costs of implementation, as well as the risk for the Data Subjects. These Technical and Organizational Security Measures are subject to change, particularly as a result of technical progress, and Provider may modify the Technical and Organizational Security Measures provided that the security of the Services provided under the Agreement and the agreed level of protection are not materially reduced. Customer confirms that the Technical and Organizational Security Measures provide an appropriate level of protection for its Personal Data.

4.4 Provider assists the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor, in particular shall:

1. (a) Keep a written record of the categories of Processing activities carried out on behalf of Customer if this obligation is applicable under Article 30 of the GDPR;
- (b) Inform Customer:
 - 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 criminal law to preserve the confidentiality of a law enforcement investigation;
 - ii. about any requests, inquiries, or complaints received directly from Data Subjects without responding to those requests unless it has been otherwise authorized in writing by Customer to do so;
 - iii. if Provider is required pursuant to European Union (EU) or Member State law to which Provider is subject to Process the Personal Data beyond the instructions from Customer before carrying out such Processing beyond the instruction, unless that EU or Member State law prohibits such information on important grounds of public interest, such notification shall specify the legal requirement under such EU or Member State Law;
- (c) Assist Customer with any Data Protection Impact Assessment as required by Article 35 of the GDPR and/or any prior consultation as required by Article 36 of the GDPR taking into account the nature of Processing and the information available to Provider that relates to the Services provided by Provider to Customer and the Personal Data Processed by Provider on behalf of Customer;
- (d) On written request of Customer or to the extent that Provider is required to do so under the Applicable Data Protection Law, correct or erase Personal Data Processed under this DPA.

4.5 Provider shall notify Customer without undue delay after Provider becomes aware of a Data Breach at Provider impacting Customer Personal Data. This notification will be sent by Provider to the signatory of the Agreement and will contain all information available to Provider, as per Article 33, 34 of the GDPR, to document the Data Breach.

5. SUB-PROCESSORS

5.1 Subject to the terms of this Section 5 and Section 6 below, Customer authorizes Provider to engage Sub-processors that may have access to Customer Personal Data for the provision of Services on Provider's behalf. Customer acknowledges and accepts that (a) Provider Affiliates may be retained as Sub-processors, including those identified in the Schedule Description of Personal Data Processing; and (b) Provider and its Affiliates respectively may engage third party Sub-processors in connection with the provision of the Services, a list of which is available in the Schedule Description of Personal Data Processing to this DPA.

5.2 All Sub-processors are required to abide by substantially the same obligations as Provider under this DPA as applicable to their performance of the Services. Provider shall remain liable to Customer for the failure of a Sub-processor to perform in accordance with its obligations. Where a Provider Affiliate is retained as a Sub-processor, an intra-group transfer agreement is in place within the Wolters Kluwer group to ensure that the sharing and where applicable, the transfer of Personal Data among Provider Affiliates comply with the Applicable Data Protection Law. Where a third party is retained as a Sub-processor, Provider or its Affiliates will ensure that such Sub-processor agrees to a contract containing the applicable data protection obligations meeting the requirements of Article 28(3), 28(4) and, where applicable, Chapter V of the GDPR as applicable, and Provider or its Affiliates shall ensure that the third party Sub-processor provides sufficient guarantees as to the application of the Technical and Organizational Measures that are relevant to the Services provided by such Sub-processor.

5.3 Provider shall inform Customer of any change regarding the addition or replacement of a Sub-processor, specifying the identity of the intended Sub-processor and the Processing activities being subcontracted ("Sub-processor Notice"). Customer shall have fourteen (14) days following the Sub-processor Notice to submit its objections specifying the reason for objecting. If Customer makes an objection within that period, Provider will make reasonable efforts to accommodate changes in Services to avoid Processing of Personal Data by the objected-to new or additional Sub-processor. If this is not possible, Customer may (i) confirm its agreement to the choice of the Sub-processor previously objected to or (ii) terminate the Agreement in whole or in part with at least three (3) months' written notice to Provider without this termination giving rise to compensation (except for the refund of fees already paid) to Customer.

6. DATA TRANSFER

6.1 Customer acknowledges that Provider may disclose Personal Data to third parties including its Sub-processors, regulators and any party based in any jurisdiction including a jurisdiction outside the EEA provided that such disclosure is required in connection with the purposes of this DPA and is in compliance with the Applicable Data Protection Law and the provisions of this DPA. If necessary, Provider individually and/or the Parties together will enter into the EU Standard Contractual Clauses and/or implement other appropriate safeguards as required by Applicable Data Protection Law.

6.2 Customer acknowledges and agrees that Customer is responsible and liable for its Affiliates, its independent contractors and Users in Third Countries, and any transfer of Personal Data to them and any further processing by them. Such transfers initiated by Customer (e.g., by creating User accounts intended for use by such Affiliates/Users), if any, shall take place under the sole responsibility of Customer and these Users. Customer acknowledges and agrees that Provider does not exercise and cannot exercise any control over such transfers. Customer warrants that it shall in this event take all necessary measures with these Affiliates, independent contractors, and Users to comply with Applicable Data Protection Law.

6.3 If Customer is itself established in a Third Country, or if Customer requests Provider to provide access to and/or a copy of the Personal Data to one or more specified Affiliates in Third Countries and Provider directly assists or intervenes in such transfer(s), Parties and where relevant Customer's Affiliates will enter into the EU Standard Contractual Clauses and/or implement other appropriate safeguards as required by Applicable Data Protection Law. Any other transfers to Third Countries other than as described in this Section 6.3, or any further transfers of the Personal Data by Customer or the aforementioned Customer Affiliates shall fall under the sole responsibility of Customer, its Affiliates and Users in accordance with Section 6.2 above (unless and to the extent Section 6.1 above applies).

7. INSPECTIONS AND AUDITS

Provider makes available to Customer all information in its possession necessary to demonstrate compliance with the obligations provided for in this DPA. Additional information (except to the extent that it is confidential to Provider or subject to trade secret) shall be provided to Customer upon written request. If the above information is insufficient to enable Customer to demonstrate that Provider complies with its compliance obligations, the Parties may agree on the terms of an additional inspection. Customer is aware that any in-person on-site audits may disturb Processor's business operations and may entail high expenditure in terms of cost and time. Customer hereby instructs Provider to carry out the controls and audits at the Sub-processors, and Provider shall provide Customer with the information concerning the Sub-processors necessary to demonstrate compliance with the obligations referred to herein and in Article 28 GDPR. Customer may address in writing to Provider such questions and requests as it deems necessary.

Furthermore, in the event of inspections or other inquiries by a Supervisory Authority, the Parties undertake to cooperate with

each other and with the Supervisory Authority and to provide each other with the necessary information.

8. EFFECTS OF TERMINATION OF THE AGREEMENT

Upon termination of the Agreement, for any reason whatsoever, Provider shall, at Customer's option, delete all Personal Data or return them to Customer (in compliance with the reversibility services agreed upon) and delete all existing copies unless Provider is required to retain such Personal Data under EU or Member State legislation.