Data Processor Agreement Wolters Kluwer Tax and Accounting B.V.

Product 'Twinfield Boekhouden' (Twinfield Accounting), 'Twinfield Samenwerken' (Twinfield Cooperation), Twinfield Consultancy

Versie: juni 2023

Wolters Kluwer

>>

DPA Wolters Kluwer Tax and Accounting B.V.

Producten Twinfield Boekhouden, Twinfield Samenwerken, Twinfield Consultancy.

The undersigned:

Wolters Kluwer Tax and Accounting Nederland B.V, a company incorporated under the laws of The Netherlands, having its registered office at De Beek 9, 3871MS Hoevelaken (hereinafter to be referred to as "**the Processor**"),

and

<Name client>, a company incorporated under the laws of [The Netherlands], having its registered office at <address client> (hereinafter to be referred to as "**the Controller**"),

hereinafter jointly also to be referred to as the "**Parties**" and each separately as a "**Party**";

Declare to have agreed as follows:

Preamble

Whereas, Parties have agreed that the Controller will use <description service> of Processor. Processer processes personal data of the controller in the context of the execution of the agreement

Now, therefore, and in order to enable the Parties to carry out their relationship in a manner that is compliant with law, the Parties have entered into this Data Processing Agreement ("DPA") as follows:

1. Definitions

For the purposes of this DPA:

"Applicable Data Protection Law":
the General Data Protection Regulation (EU) 2016/679 protecting the fundamental rights and freedoms of individuals and in particular their right to privacy with respect to the Processing of Personal Data applicable to the Controller and the Processor, and additional rules and implementations of EU data protection laid down in European member state law; the term Applicable Data Protection Law shall encompass the GDPR, effective as per 25 May 2018;

"Controller":
shall mean <name client> who determines as a natural or legal person alone or jointly with others the purposes and means of the Processing of Personal Data;

"General Data Protection Regulation" or "GDPR":
shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data which came into effect on May 25, 2018;

"International Organization":
shall mean an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

"Member State":
shall mean a country belonging to the European Union;

"Personal Data":
shall mean any information relating to an identified or identifiable natural person (Data Subject);

"Data Subject":

shall mean an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Personal Data Breach":

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

"Process/Processing":

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

"Processor":

shall mean Wolters Kluwer Tax and Accounting B.V. who Processes Personal Data on behalf of the Controller;

"Services Agreement":

shall mean the contract concluded between the Controller and the Processor setting out the terms and conditions for the provision of the Services;

"Services":

shall mean the services provided by the Processor to the Controller and described under 'subject-matter of the processing' in Annex 1 (in Dutch) of this DPA;

"Special Categories of Data":

shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data, biometric data Processed for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation;

"Sub-processor":

shall mean any data processor engaged by the Processor who agrees to receive from the Processor Personal Data exclusively intended for Processing activities to be carried out on behalf of the Controller in accordance with its instructions, the terms of this DPA and the terms of a written subcontract;

"Supervisory Authority":

shall mean an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;

"Technical and Organizational Security Measures":

shall mean those measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing; and

"Third Country":

shall mean a country where the European Commission has not decided that the country, a territory or one or more specified sectors within that country, ensures an adequate level of protection.

2. Details of the Processing

The details of the Processing operation provided by the Processor to the Controller as a commissioned data processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Annex 1 to this DPA.

3. Rights and Obligations of Controller

The Controller remains the responsible data controller for the Processing of the Personal Data as instructed to the Processor based on the Services Agreement, this DPA and as otherwise instructed. The Controller has instructed and throughout the duration of the commissioned data processing will instruct the Processor to Process the Personal Data only on Controller's behalf and in accordance with the Applicable Data Protection Law, the Services Agreement, this DPA and Controller's instructions. The Controller is entitled and obliged to instruct the Processor in connection with the Processing of the Personal Data, generally or in the individual case. Instructions may also relate to the correction, deletion, blocking of the Personal

Data. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by the Controller in writing without delay. To the extent that the implementation of an instruction results in costs for the Processor, the Processor will first inform the Controller about such costs. Only after the Controller's confirmation to bear such costs for the implementation of an instruction, the Processor is required to implement such instruction.

4. Obligations of Processor

The Processor shall:

a. process the Personal Data only as instructed by the Controller and on the Controller's behalf; such instruction is provided in the Services Agreement, this DPA and otherwise in documented form as specified in clause 3 above. Such obligation to follow the Controller's instruction also applies to the transfer of the Personal Data to a Third Country or an International Organization.

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

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

d. implement the Technical and Organizational Security Measures which will meet the requirements of the Applicable Data Protection Law as further specified in Annex 2 (in Dutch) before Processing of the Personal Data and ensure to provide sufficient guarantees to the Controller on such Technical and Organizational Security Measures.

e. assist the Controller by appropriate Technical and Organizational Measures, insofar as this is feasible, for the fulfillment of the Controller's obligation to respond to requests for exercising the Data Subjects rights concerning information, access, rectification and erasure, restriction of processing, notification, data portability, objection and automated decision-making; to the extent such feasible Technical and Organizational Measures require changes or amendments to the Technical and Organizational Measures specified in Annex 2, the Processor will advise the Controller on the costs to implement such additional or amended Technical and Organizational Measures. Once the Controller has confirmed to bear such costs, the Processor will implement such additional or amended Technical and Organizational Measures to assist the Controller to respond to Data Subject's requests.

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

g. notify Controller without undue delay:

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

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

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

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

V after the Processor becomes aware of a Personal Data Breach at the Processor. In case of such a Personal Data Breach, the Processor upon the Controller's written request will assist the Controller with the Controller's obligation under Applicable Data Protection Law to inform the data subjects and the Supervisory Authorities, as applicable, and to document the Personal Data Breach.

h. assist the Controller with any Data Protection Impact Assessment as required by Art. 35 of the GDPR that relates to the Services provided by the Processor to the Controller and the Personal Data processed by the Processor on behalf of the Controller.

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

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

6. Sub-processing

a. Processor uses general Sub-processors, i.e. no customer specific Sub-processors. The Controller authorizes the use of Sub-processor(s) engaged by the Processor for the provision of the Services. The Controller approves the following Sub-processor(s) as specified on https://taxnl.wolterskluwer.com/algemene-voorwaarden/subverwerkers.

b. In case the Processor intends to engage new or additional Sub-processors, the Processor shall update https://taxnl.wolterskluwer.com/algemene-voorwaarden/subverwerkers to reflect changes concerning the addition or replacement of any Sub-processor. Controller shall periodically check https://taxnl.wolterskluwer.com/algemene-voorwaarden/subverwerkers. If the Controller has a reasonable basis to object to the use of any such new or additional Sub-processor, the Controller shall notify the Processor promptly in writing within 14 days after Controller took notice thereof. In the event the Controller objects to a new or additional Sub-processor, and that objection is not unreasonable, the Processor will use reasonable efforts to make available to the Controller a change in the Services or recommend a commercially reasonable change to the Controller's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new or additional Sub-processor without unreasonably burdening the Controller. If the Processor is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, the Controller may terminate the effected part of the Services Agreement with respect only to those Services which cannot be provided by the Processor without the use of the objected-to new or additional Sub-processor by providing written notice to the Processor.

c. The Processor shall impose the same data protection obligation as set out in this DPA on any Sub-processor by contract. The contract between the Processor and the Sub-processor shall in particular provide sufficient guarantees to implement the Technical and Organizational Security Measures as specified in Annex 2, to the extent such Technical and Organizational Security Measures are relevant for the services provided by the Sub-processor.

d. The Processor shall choose the Sub-processor diligently.

e. If such a Sub-processor is located in a Third Country, the Processor shall, at the Controller's written request, enter into an EU model contract (Controller > Processor) on the Controller's behalf (in the Controller's name), or take other equivalent measures for the protection of Personal Data. In this case the Controller instructs and authorises the Processor to give Sub-processors instructions on the Controller's behalf and to make use of all the Controller's rights vis-à-vis the Sub-processors on the basis of the EU model contract or the other measures taken.

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

6. Limitation of liability

Any liability arising out of or in connection with this DPA shall follow, and be exclusively governed by, the liability provisions set forth in, or otherwise applicable to, the Services Agreement. Therefore, and for the purpose of calculating liability caps and/or determining the application of other limitations on liability, any liability occurring under this DPA shall be deemed to occur under the relevant Services Agreement.

7. Duration and termination

a. The term of this DPA is identical with the term of the relevant Services Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the relevant Services Agreement.

b. The Processor shall, at the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of Services, and delete any existing copies unless EU or Member State law requires the Processor to retain such Personal Data.

8. Miscellaneous

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

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

c. This DPA shall be governed by the same law as the Services Agreement except to the extent that mandatory Applicable Data Protection Law applies.

Annex 1 - Product description client

De doorgegeven Persoonsgegevens betreffen de volgende categorieën Betrokkenen:

- Klanten van Verantwoordelijke
- Werknemers van Verantwoordelijke
- Leveranciers van Verantwoordelijke

Onderwerp van de verwerking

Gebruik van boekhoudsoftware

Aard en doel van de verwerking

Verwerker verzamelt, verwerkt en gebruikt de Persoonsgegevens van de Betrokkenen ten behoeve van Verantwoordelijke teneinde uitvoering van de overeenkomst.

Soort persoonsgegevens

De Persoonsgegevens die door Verwerker ten behoeve van Verantwoordelijke zijn verzameld, verwerkt en gebruikt betreffen de volgende categorieën persoonsgegevens: financiële gegevens en contactgegevens

Contactgegevens in geval van datalekken

Verwerker : Richard Ridderhof, NL-TAA-Compliance@wolterskluwer.com

Annex 2 - Security measures

Beschrijving van de Technische en Organisatorische Beveiligingsmaatregelen die door Verwerker zijn doorgevoerd in overeenstemming met Toepasselijke Gegevensbeschermingswet:

In deze Bijlage worden de Technische en Organisatorische Beveiligingsmaatregelen en procedures beschreven die Verwerker ten minste moet aanhouden ter bescherming van de veiligheid van persoonsgegevens die zijn gecreëerd, verzameld, ontvangen, of anderszins verkregen.

Algemeen: Technische en organisatorische maatregelen kunnen worden beschouwd als de stand der techniek op het moment van sluiten van de Overeenkomst van Dienstverlening. Verwerker zal technische en organisatorische maatregelen na verloop van tijd evalueren, daarbij rekening houdend met kosten voor doorvoering, aard, omvang, context en doelstellingen van verwerking, en het risico van verschillen in de mate van waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen.

Gedetailleerde technische maatregelen:	Voorstel Verwerker:	Modulariteit/ Optionaliteit	Beschikbare certificering
Pseudonimisering van gegevens	Bij bijzondere persoonsgegevens	Gedeeltelijk	ISAE 3402 type 2
Encryptie van gegevens	Bij bijzondere persoonsgegevens	Gedeeltelijk	ISAE 3402 type 2
Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen	Aanwezig		ISAE 3402 type 2
Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident	Aanwezig		ISAE 3402 type 2
Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen.	Aanwezig		ISAE 3402 type 2