BASECONE DATA PROCESSING AGREEMENT (BASECONE AS PROCESSOR)

The undersigned:

Basecone N.V., a corporation established under Dutch law, with its corporate domicile at Eemweg 8, 3742 LB Baarn, the Netherlands and listed in the Commercial Register of the Chamber of Commerce under number 55299245 (**"the Processor"**),

and

_____ Controller's name _____ a corporation established under _____ country adjective _____, law, with its corporate domicile at _____ address and housenumber _____, _____ zipcode _____ _____ town/city _____ and listed in the Commercial Register of the Chamber of Commerce under number _____ CoC number _____ (**"the Controller"**),

referred to jointly below as the "**Parties**" and each separately as a "**Party**",

declare that they have agreed as follows:

WHEREAS:
The Parties agree that the Controller shall use the Processor as the supplier of accounting software. The Processor shall process personal data of the Controller for the purpose of performing the agreement.

To enable the Parties to give effect to their relationship in a legally compliant manner, they have entered into this Data Processing Agreement ("DPA") as follows:

1. Definitions

The following terms have the stated meaning in this DPA:

"Applicable Data Protection Law"	the legislation that provides protection for the fundamental rights and freedoms of people, in particular their right to privacy in relation to the Processing of Personal Data, which legislation applies to the Controller and Processor; the term Applicable Data Protection Law also includes the GDPR once this enters into force on May 25, 2018;
"Controller"	the aforementioned client of Basecone, which as a natural person or legal entity, alone or jointly with others, determines the purpose and means of the Processing of Personal Data;
"General Data Protection Regulation" or "GDPR"	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. The GDPR enters into force on May 25, 2018;
"International Organization"	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"	a country that belongs to the European Union;
"Personal Data"	any information relating to an identified or identifiable natural person (Data Subject);
"Data Subject"	an identifiable natural 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"	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;
"Process/Processing"	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"	Basecone N.V., which processes Personal Data on behalf of the Controller;
"Agreement between the client and Basecone on taking out a Subscription"	the main agreement between the Controller and Processor that sets out the conditions for the provision of the Services;
"Services"	the services provided by the Processor to the Controller and described under "subject matter of the processing" in Appendix 1 to this DPA;
"Special Categories of Personal Data"	personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; the Processing of genetic data and biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation;
"Subprocessor"	a data processor engaged by the Processor that declares its willingness to receive Personal Data from the Processor intended solely for Processing Activities that must be performed for the Controller in accordance with its instructions, the conditions of this DPA, and the conditions of a written subprocessing agreement;
"Supervisory Authority"	an independent public authority which is established by a Member State pursuant to Article 51 GDPR;
"Technical and Organizational Security Measures"	the measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, unauthorized disclosure or access, particularly when the Processing involves transmitting data via a network, and against all other unlawful forms of Processing.

"Third Country"	a country in respect of which the European Commission has not found that that country, a territory, or one or more specified sectors within that country ensure an adequate level of data protection.

2. Details of the Processing

The details of the Processing Activities that the Processor performs for the Controller as a data processor that has received instructions to that effect (such as the subject matter, the nature, and the purpose of the processing, the type of personal data, and the categories of data subjects) are set out in Appendix 1 to this DPA.

3. Rights and obligations of the Controller

The Controller remains the responsible data controller for the Processing of the Personal Data in accordance with the instructions to the Processor under the [Agreement for Services], this DPA, and any further instructions. The Controller has instructed the Processor, and shall continue to instruct the Processor for the duration of the data processing for which the instruction has been given, to process the Personal Data solely for the Controller and in accordance with the Applicable Data Protection Law, the Agreement between the client and Basecone on taking out a Subscription, this DPA, and the Controller's instructions. The Controller is entitled and obliged to give the Processor instructions for the Processing of the Personal Data, both in general and in individual cases. Instructions can also relate to the rectification, deletion, and blocking of Personal Data. Instructions are generally given in writing, unless urgency or other specific circumstances require a different form (e.g. oral or electronic). The Controller shall immediately confirm unwritten instructions in writing. Insofar as carrying out an instruction leads to costs for the Processor, the Processor shall first notify the Controller of those costs. The Processor shall carry out an instruction only once the Controller has confirmed that it is responsible for the costs of carrying out that instruction.

4. Obligations of the Processor

The Processor shall:

a) process the Personal Data solely in accordance with the Controller's instructions and for the Controller; the instructions are given in the Agreement between the client and Basecone on taking out a Subscription, this DPA, and otherwise in documented form as set out in Article 3 above. The obligation to follow the Controller's instructions also applies to the transmission of the Personal Data to a Third Country or an International Organization;

(b) immediately inform the Controller if it cannot comply with an instruction of the Controller for whatever reason;

(c) ensure that persons it authorizes to Process the Personal Data for the Controller undertake to maintain confidentiality or that those persons are subject to an appropriate obligation of secrecy, and that the persons who have access to the Personal Data will Process those Personal Data in accordance with the Controller's instructions;

(d) implement the Technical and Organizational Security Measures that comply with the requirements of the Applicable Data Protection Law, as further specified in Appendix 2, before Processing the Personal Data and shall ensure that it gives adequate guarantees to the Controller as regards the Technical and Organizational Security Measures;

(e) assist the Controller by means of appropriate Technical and Organizational Measures, insofar as feasible, for the fulfillment of the Controller's obligation to respond to requests from Data Subjects to exercise their rights relating to information, access, rectification and deletion, restriction of processing, notification, data portability, making objections, and automated decision-making; insofar as those feasible Technical and Organizational Measures require changes or alterations to the Technical and Organizational Measures set out in Appendix 2, the Processor shall inform the Controller of the costs of implementing those additional or altered technical and Organizational Measures. As soon as the Controller has confirmed that it is responsible for those costs, the Processor shall implement the additional or altered Technical and Organizational measures to assist the Controller in ensuring compliance with data subjects' requests;

(f) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and Article 28 GDPR, and allow for and contribute to audits, including inspections conducted by the controller or another auditor mandated by the Controller. The Controller is aware that audits in person and on location can significantly disrupt the Processor's business operations, cost a lot of money, and be time-consuming. Accordingly, the Controller may conduct an audit in person and on location only if it reimburses the costs incurred by the Processor due to the disruption of its business operations;

(g) notify the Controller without unnecessary delay:

(i) of any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless this notice is otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) of complaints and requests received directly from Data Subjects (for example, complaints and requests relating to access, rectification, deletion, restriction of processing, notification, data portability, objections against data processing, and automated decision-making) without dealing with that request further unless it is otherwise authorized to do so;

(iii) if the Processor is obliged on the basis of EU legislation or the legislation of a Member State that applies to it to process the Personal Data beyond the scope of the Controller's instructions, before carrying out that processing beyond that scope, unless the EU legislation or legislation of that Member State prohibits that information for compelling reasons of public interest; the notice must specify the statutory requirement under that EU legislation or the legislation of the Member State;

(iv) if, in the Processor's opinion, an instruction is contrary to the Applicable Data Protection Law; if it gives that notice, the Processor is not obliged to follow the instruction, unless and until the Controller has confirmed or altered it; and

(v) as soon as the Processor becomes aware of a Personal Data Breach, within no more than 24 hours. If such a Personal Data Breach occurs, the Processor shall assist the Controller, at the Controller's written request, with its obligation under the Applicable Data Protection Law to report the breach to the Data Subjects or the Supervisory Authority, and to document the Personal Data Breach. Contact details relating to the report are recorded in the client service system. The contact persons are listed in the appendix to this agreement;

(h) assist the Controller in a Data Protection Impact Assessment as required under Article 35 GDPR relating to the Services provided by the Processor to the Controller and the Personal Data that the Processor processes for the Controller;

(i) deal with all questions of the Controller relating to its Processing of the Personal Data (for example, to enable the Controller to respond promptly to complaints or requests of Data Subjects) and to comply with the advice of the Supervisory Authority on the Processing of the transmitted data;

(j) insofar as it is obliged and requested to rectify, delete, and/or block Personal Data that is processed under this DPA, do this immediately. If and insofar as Personal Data cannot be deleted because of statutory data retention requirements, the Processor, instead of deleting the relevant Personal Data, shall restrict the further Processing and/or use of the Personal Data, or remove the corresponding identity from the Personal Data ('blocking'). If such a blocking obligation applies to the Processor, the Processor shall delete the relevant Personal Data by no later than the last day of the calendar year in which the retention period ends.

6. Subprocessing ubverwerking

(a) The Controller consents to the use of the Subprocessor(s) that the Processor engages for the provision of the Services. The Controller gives its consent for the Subprocessor(s) as listed at www.basecone.com/en/privacy.

(b) If the Processor intends to engage new or more Subprocessors, it shall ensure that www.basecone.com/en/privacy is updated. The Controller shall ensure that www.basecone.com/en/privacy is periodically consulted. If the Controller has a reasonable ground on which to object to the use of new or more Subprocessors, it shall immediately notify the Processor of its objection in writing within fourteen days of receipt of the Subprocessor Notice. If the Controller objects to a new or different Subprocessor, and that objection is not unreasonable, the Processor shall reasonably endeavor to make changes in the Services available to the Controller or recommend a commercially reasonable alteration to the Controller's configuration or the Controller's use of the Services to prevent the Processing of Personal Data by the new or different Subprocessor against which the objection has been made, without unreasonably burdening the Controller in the process. If the Processor cannot make that alteration available within a reasonable period, which will not exceed sixty (60) days, the Controller may terminate the relevant portion of the [Agreement for Services], although only in relation to those services that the Processor is unable to provide without using the new or different Subprocessor against which the objection has been made, by means of a written notice to the Processor.

(c) The Processor shall contractually impose the same data protection obligation as included in this DPA on all Subprocessors. The agreement between the Processor and the Subprocessor must namely give adequate guarantees for the implementation of the Technical and Organizational Security Measures as specified in Appendix 2, insofar as those Technical and Organizational Security Measures are important for the services provided by the Subprocessor.

(d) The Processor shall choose the Subprocessor with the utmost care.

(e) If such a Subprocessor is located in a Third Country, the Processor, at the Controller's written request, shall enter into an EU model contract (Controller > Processor) on behalf of the Controller (in the Controller's name), pursuant to Commission Decision 2010/87/EU. In this case, the Controller instructs and authorizes the Processor to give Subprocessors instructions in the Controller's name and to enforce all the Controller's rights in respect of the Subprocessors under the EU model contract.

(f) The Processor remains liable toward the Controller for the fulfillment of the Subprocessor's obligations, if that Subprocessor fails to fulfill its obligations. However, the Processor is not liable for any damage/loss and claims arising from the Controller's instructions to the Subprocessors.

7. Limitation of liability

All liability arising from or relating to this DPA follows, and is exclusively governed by, the liability provisions set out in, or otherwise applicable to, the [Agreement for Services]. For this reason, and to calculate liability limits and/or determine the application of other limitations of liability, each case of liability that arises from the DPA is deemed to arise from the relevant [Agreement for Services].

8. Duration and termination

(a) The term of this DPA coincides with the term of the relevant [Agreement for Services]. Unless this agreement stipulates otherwise, rights and obligations relating to termination are the same as the rights and obligations included in the relevant [Agreement for Services].

(b) At the Controller's discretion, the Processor shall either delete all Personal Data or return all Personal Data to the Controller when it stops providing services, and delete all existing copies unless the Processor is obliged under EU legislation or the legislation of a Member State to retain those Personal Data.

9. Miscellaneous

(a) If there is any inconsistency between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA will prevail in relation to the Parties' data protection obligations. If there is any doubt about whether clauses in those other agreements relate to the Parties' data protection obligations, this DPA will prevail.

(b) The invalidity or unenforceability of any provision of this DPA has no consequences for the validity or enforceability of the other provisions of this DPA. The invalid or unenforceable provision is to be (i) amended so as to guarantee its validity and enforceability while simultaneously maintaining the Parties' intentions as far as possible or – if this is not possible – (ii) interpreted as though the invalid or enforceable part was never included in it. The above also applies if there is an omission in this DPA.

(c) This DPA is governed by the same legislation as the Agreement between the client and Basecone on taking out a Subscription except insofar as the mandatory Applicable Data Protection Law is applicable.

On behalf of the Controller:

Full name: _____

Position: _____

Address: _____

Date: _____

Signature:

On behalf of the Processor: Nico Bogaerts

Full name:

Position: Managing Director

Address: Eemweg 8, 3742 LB Baarn, the Netherlands

Date: _____

Signature:

Appendix 1 – Categories of Data Subjects

The transmitted Personal Data include the following categories of Data Subjects:

- Companies
- Customers of clients

Subject-matter of the processing

Use of invoice processing software

Nature and purpose of the processing

The Processor collects, processes, and uses the Personal Data of the Data Subjects for the Controller in order to perform the agreement.

Type of personal data

The Personal Data that the Processor collects, processes, and uses for the Controller include the following categories of personal data: financial data and contact details, more specifically:

Subscription details:

- the required subscription
- user name

Your personal data:

- sex
- first name and surname
- telephone number
- e-mail address
- name and location of your accountant

Your company details:

- legal form
- company name
- billing address
- zip code and town/city
- e-mail address

Payment details:

- IBAN and name details.

Contact persons in the event of a security breach

Controller: _____

Processor: Compliance & Privacy Manager WK TAA Europe CSO – NL-TAA-compliance@wolterskluwer.com

Appendix 2 – Security measures sheet

Description of the Technical and Organizational Security Measures that the Processor has implemented in accordance with the Applicable Data Protection Law

This Appendix describes the minimum Technical and Organizational Security Measures and procedures that the Processor must maintain to protect the security of personal data that are created, collected, received, or otherwise obtained.

General: Technical and organizational measures may be regarded as the state of the art when the Agreement for Services is concluded. The Processor shall evaluate the technical and organizational measures over the course of time, taking into account the implementation costs, nature, extent, context, and purposes of processing, as well as the risk of differences in the degree of probability and seriousness for the rights and freedoms of natural persons.

Detailed technical measures

- Logical access control to Basecone's systems, using strong passwords and a password policy:
  - Passwords are stored encrypted in our database;
  - Passwords must at least include: eight characters, one numerical value, one letter, and one special character: (! @ # $ % ^ & / ? * ( ) _ + = [ ] { } | ; : " ');
  - All Basecone employees are informed and concerned about "Social Engineering";
  - Login details are blocked after three incorrect login attempts.
- Physical access security (to the Basecone office) based on a combination of an electronic key and coded access to the office space.
- Secured network connections, using Secure Socket Layer (SSL).
- Basecone monitors its systems 24/7:
  - Availability is measured every minute from three locations around the world. Results are logged at www.basecone.com/en/status;
  - A qualified team of Operation Engineers and Developers monitors Basecone's virtual servers. It is possible to measure each machine and each service to determine whether these are available and/or render the necessary performance to comply with the agreed Service Levels. Alerts are issued via SMS and e-mail.
  - Basecone works in the cloud. This means that its Virtual Servers are available in the Data Center of Amazon Web Services (AWS) in Frankfurt. Our systems are duplicated here in what are known as "Availability Zones".
  - Basecone uses AWS's "Elastic Load Balancer". This makes it possible to determine which services must be mobilized based on demand via https://secure.basecone.com. As a result, out-of-the-box security measures, such as DDoS security, SSL security protocols, Cyphers, and Options are used directly.
  - All virtual servers remain within our own Virtual Private Cloud (VPC), with Network Access Controls (ACLs) that ensure requests arrive properly in our network.

Log files

- All user actions are logged and saved for a period of fourteen days.
- The logs consist of the following parts:
- Incoming mail: all e-mails that are imported;
- WebPortal: all actions that the user performs and all errors that result from them;
- API: all actions that the user performs and all errors that result from them.
- The following personal data are present in the logs:
  - User name
  - Office ID
  - User ID
  - IP address
  - E-mail address / full e-mail

By means of these data, it is possible to determine who the user is and what this person has done.

- As Basecone saves the “Document Workflow Status” in log files for an indefinite period, it also keeps these on record for an indefinite period. This log can thus always be used to check what actions have been performed on documents, such as delivery, deletion, splitting, merging, recording, etc. Actions that relate to users, such as name changes and granting access, are not saved in this log.

These log data are stored on the production servers in a central log database. This is not the same database as the client database. Access to both databases is required in order to know which user is involved.