DATA PROCESSING AGREEMENT
BV SPONIZA IT

Comprised of:
Part 1. Data Pro Statement
Part 2. Standard Clauses for Data Processing

Version: 1.5
Only change compared to v1.4: for merchants connecting through the indirect wisteria model (see https://faq.webwinkelfacturen.nl/content/36/286/nl/heeft-webwinkelfacturennl-een-eigen-api.html) BV Sponiza IT may store customer data for a maximum of 10 days for the sole purpose of transferring the data to the accounting / invoice systems. This will be done securely and without any other purpose. As soon as the transfer to the accounting system is successfully completed, the customer data is deleted.

PART 1: DATA PRO STATEMENT

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

GENERAL INFORMATION

1. This Data Pro Statement was drawn up by
BV Sponiza IT, a limited liability company (een besloten vennootschap met beperkte aansprakelijkheid) established under Dutch law, with its statutory office at Waldeck Pyrmontlaan 12, 2243 HM Wassenaar and registered with the chamber of commerce under number 34118277 and also doing business using the trade names '**Webwinkelfacturen.nl' or 'Winkelboekhouding.nl'**, and duly represented by ST Fischer, director, and hereinafter to be referred to as '**Sponiza'** or '**Data Processor'**

If you have any queries about this Data Pro Statement or data protection in general, please contact:
Sophie Fischer
sophie@webwinkelfacturen.nl
+31 6 54 64 52 95

2. This Data Pro Statement will enter into force on the date issued by the electronic time stamp, which can be found at the Client's dashboard.
We regularly revise the security measures outlined in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. If this document is updated, we will notify you of the revised versions through our regular channels.

3. This Data Pro Statement applies to the following products and services provided by the data processor:

Connectors between online stores (in Dutch: 'webwinkel) and/or POS and accounting or invoicing software delivered by Sponiza under the trade names **webwinkelfacturen.nl** or **winkelboekhouding.nl**

4. Description of service
The services do the following:
Retrieve sales-data from online stores and/or point of sales and transfer this data to accounting- or invoice systems. The customer selects and authorises which online store / Point of Sale and accounting- or invoice system is used.

5. Intended use: the service was designed and built to process the following types of data:
The following data is retrieved from the online store and/or point of sales:
- Sales data, including the sale-lines, the date of sale, the tax codes and prices
- Debtor information such as address details and email details
- Product details like SKU and price

Sponiza does not access the content of the data and the content of the data are out of Sponiza's scope. Sponiza only processes the data provided by its customers without accessing these. Therefore Sponiza cannot be held accountable for the content of the data and Sponiza's data processing does not categorise data in various categories. For the avoidance of doubt: the Client bears the full responsibility for the actual content of the data processed by Sponiza. **It is up to the client to determine whether or not it will use the aforementioned product or service to process such data.**

6. When the data processor designed the product or service, it applied the *privacy-by-design* approach in the following manner:
a. The connectors store as little data as possible on the platform.
b. Most data are deleted after the financial transaction is pushed to the accounting- or invoice system.
c. Sponiza is transparent regarding the data we store

d. All data pushed to accounting- and invoice systems are encrypted by means of SSL-certificates. If the online store also uses encryption, all data retrieved from these online stores is encrypted. If the online store does not use encryption, only data sent to the Sponiza platform through webhooks is encrypted.
e. Strong passwords are used. There is a limited idle time for the dashboards.
f. The only personal data that is stored concerns the email addresses of the debtor (i.e. customer of the merchant), with the sole purpose to enable sales under the same debtor (matched on the email address).
g. Sponiza does not sell any Personal Data to 3rd parties or uses the Personal Data for purposes of its own.

7. The data processor adheres to the Data Processing Standard Clauses for Data Processing

8. The data processor will process the personal data provided by its clients within the EU/EEA.

9. The data processor uses the following sub-processors:

Sponiza is not using sub- processors. However, if Sponiza wishes to do so in the future, the Client grants Sponiza a general permission for using sub-processors by signing this data processing agreement. Sponiza will duly inform the Client in advance if Sponiza starts using sub-processors and shares the business details as well as any changes therein with the client. For the avoidance of doubt: the Client will have to contract 3rd parties providing online store software, POS, accounting and invoicing software directly and independently from Sponiza. Sponiza does not regard such suppliers as sub-processors.

10. The data processor will support its clients in the following way when they receive requests from data subjects:
As Sponiza only stores two types of information, a Client sending such a request to avg@webwinkelfacturen.nl, will receive:
a. A csv-file with debtor-email addresses for his connector
b. His latest company (invoice) details on record

11. Once an agreement with a client has been terminated, the data processor will delete the personal data it processes on behalf of the client within three months, in such a manner that they will no longer be able to be used and will be rendered inaccessible. For the avoidance of doubt: the Dutch tax authorities require Sponiza to store all its tax related data for 7 years. The tax related data will be deleted within 3 months after the expiration of this mandatory storage period if the Client has terminated the service.

SECURITY POLICY

1. The data processor has implemented the following security measures to protect its product or service:

a. The email addresses will not be pseudonomisated but the email address is decoupled from the all other data so it cannot be used to retrieve a sales history.
b. Communication to and from the platform is encrypted
c. Hourly and daily backups are created for problem recovery. Backups are stored for a week maximally.
d. Strong password and long license-keys. The license key and email address and password are required to log in.
e. Wherever possible we use Oauth for the connection with external systems.
f. A specific avg email address where emails are deleted if the information is not needed anymore.
g. Database queries are created and are running via protected queries. Data input via forms is validated against special characters. We use captcha for registrations.
h. Strict server is protected by firewalls and regular analysers run to detect breaches.
I. Communication within the platform is ensured via variable signatures.

DATA LEAK PROTOCOL

1. In the unfortunate event that something does go wrong, the data processor will follow the following data breach protocol to ensure that clients are notified of incidents.

In case of a data breach:

If Sponiza establishes a data breach, Sponiza will contact the Client's contact person for such events. The Client has provided Sponiza with the relevant contact details and is responsible for keeping these up to date and sharing the updated contact details with Sponiza.

If, according to Sponiza, a data breach in accordance with the GDPR (in Dutch: AVG) can be established, Sponiza will provide the Client with the following information relating to the data breach and will also inform the Autoriteit Persoonsgegevens ('**AP**') if so required by the GDPR:

Contact details Sponiza:

Sophie Fischer, director; sophie@webwinkelfacturen.nl; + 31 6 54 64 52 95

Details of the data breach

- Sponiza provides an incident summary relating to the security breach affecting the infringement of the Personal Data.

- Of how many people were the Personal Data infringed by the data breach ? [fill

out the numbers] or minimally: [#]) and maximally: [#]

- Describe the group of people whose Personal Data were involved with the data breach.

- When did the data breach occur? (choose 1 option and complete if necessary.): (i) at [date] or (ii) between [starting date period] and [end date period] or (iii) yet unknown.

- What type of data breach occurred ? Erase what is inapplicable: (i) reading (confidentiality), (ii) copying, (iii) altering (integrity), (iv) deleting or destroying (availability), (v) theft, (vi) yet unknown.

- What type of Personal Data are involved ? Erase what is inapplicable: (i) name -, address – and place of living details, (ii) phone numbers, (iii) e-mail addresses or other addresses used for electronic communication, (iv) access or identification data (e.g. username/password or customer number), (v) financial data (e.g. bank account number, credit card number), (vi) Civil service number (BSN) ,(vii) copies of passports or copies of other ID cards, (viii) gender, date of birth and/or age.

Data breach follow-up

Sponiza will endeavour to render advice on preventing future Data breaches. The aborted connection will only be reinstated if the data breach has been solved and upon receipt of the Client's explicit permission.

Technical prevention

- Have the Personal Data been encrypted, hashed or otherwise been made inaccessible or incomprehensible for unauthorised 3rd parties ? Erase what is inapplicable: (i) yes (ii) no (iii) partly, being: [complete]

- If the Personal Data have been made inaccessible or incomprehensible, whether partly or in full, describe the method used ? (This question should be answered if you didn't erase option i or iii in the previous question. If encryption was used, please elaborate on the encryption method).

International aspects

• Does the Data Breach involve people in other EU countries? Erase what is inapplicable (i) yes, (ii) no, (iii) yet unknown.

PART 2: STANDARD CLAUSES FOR DATA PROCESSING

Version: January 2018

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the services documentation and to the appendices thereof, e.g. any general terms and conditions that may apply.

ARTICLE 1. DEFINITIONS

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the regulatory agency outlined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation (in Dutch: AVG).

1.3 **Data Processor**: the party which, in its capacity as an ICT supplier, processes Personal Data on behalf of its Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: a statement issued by the Data Processor in which it provides information on the intended use of its product or service, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects, among other things.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf the Data Processor processes Personal Data. The Client may be either the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between the Client and the Data Processor, on whose basis the ICT supplier provides services and/or products to the Client, the data processing agreement being part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as outlined in Article 4.1 of the GDPR, processed by the Data Processor to meet its requirements under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, along with the Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

ARTICLE 2. GENERAL PROVISIONS

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by the Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of the Client's data processing agreements is expressly rejected.

2.2 The Data Pro Statement, and particularly the security measures outlined in it, may be adapted from time to time to changing circumstances by the Data Processor. The Data Processor will notify the Client in the event of significant revisions. If the Client cannot reasonably agree to the revisions, the Client will be entitled to terminate the data

processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions. Terminating the data processing agreement also results in simultaneously terminating the service between the Client and Sponiza in accordance with the applicable articles in the general terms and conditions

2.3 The Data Processor will process the Personal Data on behalf and on behalf of the Client, in accordance with the written instructions provided by the Client and accepted by the Data Processor.

2.4 The Client or its customer will serve as the controller within the meaning of the GDPR, will have control over the processing of the Personal Data and will determine the purpose and means of processing the Personal Data.

2.5 The Data Processor will serve as the processor within the meaning of the GDPR and will therefore not have control over the purpose and means of processing the Personal Data, and will not make any decisions on the use of the Personal Data and other such matters.

2.6 The Data Processor will give effect to the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to the Client to judge, on the basis of this information, whether the Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures so as to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 The Client will guarantee to the Data Processor that it acts in accordance with the GDPR, that it provides a high level of protection for its systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on the Client by the Dutch Data Protection Authority will not be able to be recouped from the Data Processor, except in the event of wilful misconduct or gross negligence on the part of the Data Processor's management team.

ARTICLE 3. SECURITY

3.1 The Data Processor will implement the technical and organisational security measures outlined in its Data Pro Statement. In implementing the technical and organisational security measures, the Data Processor will take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing operations and the intended use of its products and services, the risks inherent in processing the data and risks of various degrees of likelihood and severity to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of the Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the product or service provided by the Data Processor will not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 The Data Processor seeks to ensure that the security measures it will implement are appropriate for the manner in which the Data Processor intends to use the product or service.

3.4 In the Client's opinion, said security measures provide a level of security that is tailored to the risks inherent in the processing of the Personal Data used or provided by the Client, taking into account the factors referred to in Article 3.1.

3.5 The Data Processor will be entitled to adjust the security measures it has implemented if it feels that such is necessary for a continued provision of an appropriate level of security. The Data Processor will record any significant adjustments it chooses to make, e.g. in a revised Data Pro Statement, and will notify the Client of said adjustments where relevant.

3.6 The Client may request the Data Processor to implement further security measures. The Data Processor will not be obliged to honour such requests to adjust its security measures. If the Data Processor makes any adjustments to its security measures at the Client's request, the Data Processor will be allowed to invoice the Client for the costs associated with said adjustments. The Data Processor will not be required to actually implement these security measures until both Parties have agreed in writing and signed off on the security measures requested by the Client.

ARTICLE 4. DATA BREACHES

4.1 The Data Processor does not guarantee that its security measures will be effective under all conditions. If the Data Processor discovers a data breach within the meaning of Article 4.12 of the GDPR, it will notify the Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which the Data Processor will notify the Client of data breaches.

4.2 It is up to the Controller (the Client or its customer) to assess whether the data breach of which the Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (the Client or its customer) will at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. The Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, the Data Processor will provide more information on the data breach and will help the Client meet its breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information.

4.4 If the Data Processor incurs any reasonable costs in doing so, it will be allowed to invoice the Client for these, at the rates applicable at the time.

ARTICLE 5. CONFIDENTIALITY

5.1 The Data Processor will ensure that the persons processing Personal Data under its responsibility are subject to a duty of confidentiality.

5.2 The Data Processor will be entitled to furnish third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or legal order to do so issued by a government agency.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by the Data Processor to the Client, and any and all information provided by the Data Processor to the Client which gives effect to the

technical and organisational security measures included in the Data Pro Statement are confidential and will be treated as such by the Client and will only be disclosed to authorised employees of the Client. The Client will ensure that its employees comply with the requirements outlined in this article.

ARTICLE 6. TERM AND TERMINATION

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and will enter into force at the time of the conclusion of the Agreement and will remain effective until terminated.

6.2 This data processing agreement will end by operation of law when the Agreement or any new or subsequent agreement between the parties is terminated.

6.3 If the data processing agreement is terminated, the Data Processor will delete all Personal Data it currently stores and which it has obtained from the Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data will no longer be able to be used and will have been *rendered inaccessible*.

6.4 If the Data Processor incurs any costs associated with the provisions of Article 6.3, it will be entitled to invoice the Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if the Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such cases, the Data Processor will only continue to process the Personal Data insofar as such is necessary by virtue of its statutory obligations. Furthermore, the provisions of Article 6.3 will not apply if the Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

ARTICLE 7. THE RIGHTS OF DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENTS (DPIA) AND AUDITING RIGHTS

7.1 Where possible, the Data Processor will cooperate with reasonable requests made by the Client relating to Data Subjects claiming alleged rights from the Client. If the Data Processor is directly approached by a Data Subject, it will refer the Data Subject to the Client where possible.

7.2 If the Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, the Data Processor will cooperate with such, following a reasonable request to do so.

7.3 The Data Processor will be able to demonstrate its compliance with its requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.4 In addition, at the Client's request, the Data Processor will provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, the Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, the Client will be entitled to have an audit performed (at its own expense) not

more than once every year by an independent, fully certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The audit will be limited to verifying that the Data Processor is complying with the arrangements made regarding the processing of the Personal Data as laid down in the present data processing agreement. The expert will be subject to a duty of confidentiality with regard to his/her findings and will only notify the Client of matters that cause the Data Processor to fail to comply with its obligations under the data processing agreement. The expert will furnish the Data Processor with a copy of his/her report. The Data Processor will be entitled to reject an audit or instruction issued by the expert if it feels that the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures it has implemented.

7.5 The parties will consult each other on the findings of the report at their earliest convenience. The parties will implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. The Data Processor will implement the proposed measures for improvement insofar as it feels these are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.

7.6 The Data Processor will be entitled to invoice the Client for any costs it incurs in implementing the measures referred to in this article.

ARTICLE 8. SUB-PROCESSORS

1. The Data Processor has outlined in the Data Pro Statement whether the Data Processor uses any third parties (sub-processors) to help it process the Personal Data, and if so, which third parties.
2. The Client authorises the Data Processor to hire other sub-processors to meet its obligations under the Agreement.
3. The Data Processor will notify the Client if there is a change with regard to the third parties hired by the Data Processor, e.g. through a revised Data Pro Statement. The Client will be entitled to object to the aforementioned change implemented by the Data Processor. The Data Processor will ensure that any third parties it hires will commit to ensuring the same level of Personal Data protection as the security level the Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

ARTICLE 9. OTHER PROVISIONS

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the services documentation. Therefore, any and all rights and requirements arising from the services documentation, including any general terms and conditions and/or limitations of liability, which may apply, will also apply to the data processing agreement.