Data Processing Agreement

Version 1.2 - 16 Dec 2019

Instruction (not part of this agreement): you are kindly requested to fill out the yellow fields (on pages 1 and 6). Please return a signed copy and keep one for your own administration.

This data processing agreement is part of all agreements between the two parties mentioned below and will be referred to hereinafter as “the Agreement”.

The parties,

– **[Your company name:] ……………………………..**, a company having its principle place of business in [ADDRESS] …………………………………, registered with the Chamber of Commerce under number [Chamber of Commerce number of your company] …………………………………, hereby duly represented by [your personal name] …………………………………, (hereinafter: ‘the Controller’);

– **PestScan,** a company having its principle place of business in *Leeghwaterstraat 25, 2811 DT Reeuwijk, the Netherlands,* registered with the Chamber of Commerce under number 73105511, hereby duly represented by J.C. Smits, (hereinafter: ‘the Processor’);

hereinafter collectively referred to as ‘Parties’ and individually ‘Party’,

having regard to the fact that,

- the Controller has access to the personal data of various clients (hereinafter: ‘Data subjects’);
- the Controller wants the Processor to execute certain types of processing in accordance with the agreement concluded with the Processor (hereinafter: ‘the Agreement’);
- the Controller has determined the purpose of and the means for the processing of personal data as governed by the terms and conditions referred to herein;
- the Processor has undertaken to comply with this data processing agreement (hereinafter: ‘the Data Processing Agreement’) and to abide by the security obligations and all other aspects of the General Data Protection Regulation Act (hereinafter: ‘GDPR’);
- the Controller is hereby deemed to be the responsible party within the meaning of the GDPR;
- the Processor is hereby deemed to be the processor within the meaning of the GDPR;
- the Parties, having regard also to the provisions of the GDPR, wish to lay down their rights and duties in writing in this Data Processing Agreement,

have agreed as follows,

ARTICLE 1. PROCESSING OBJECTIVES

1.1. The Processor undertakes to process personal data on behalf of the Controller in accordance with the conditions laid down in this Data Processing Agreement. The processing will be executed exclusively within the framework of the Agreement, and for all such purposes as may be agreed to subsequently.

1.2. The Processor shall refrain from making use of the personal data for any purpose other than as specified by the Controller. The Controller will inform the Processor of any such purposes which are not contemplated in this Data Processing Agreement.

1.3. All personal data processed on behalf of the Controller shall remain the property of the Controller and/or the relevant Data subjects.

1.4. The Processor shall take no unilateral decisions regarding the processing of the personal data for other purposes, including decisions regarding the provision thereof to third parties and the storage duration of the data. The controller indemnifies the Processor against all claims that are related to the incorrect compliance with this registration obligation.

ARTICLE 2. PROCESSOR'S OBLIGATIONS

2.1. The Processor shall warrant compliance with the applicable laws and regulations, including laws and regulations governing the protection of personal data, such as the GDPR.

2.2. The Processor shall furnish the Controller promptly on request with details regarding the measures it has adopted to comply with its obligations under this Data Processing Agreement and the GDPR.

2.3. The Processor's obligations arising under the terms of this Data Processing Agreement apply also to whomsoever processes personal data under the Processor's instructions.

2.4. The Processor will notify the Controller if, in her opinion, an instruction by the Controller is in conflict with relevant privacy laws and regulations.

2.5. The Processor will provide the Controller with the necessary cooperation if a data protection impact assessment, or prior consultation of the supervisor, is necessary in the context of the processing. Any costs involved, are for the Controller.

ARTICLE 3. TRANSMISSION OF PERSONAL DATA

3.1. The Processor may process the personal data in countries inside the European.

3.2. The Processor shall notify the Controller as to which country or countries the personal data will be processed in. PestScan is hosted on a server in the Netherlands.

3.3. Articles 3.1 and 3.2 do not apply to your situation, if you run PestScan on a server that is owned and/or controlled by you.

ARTICLE 4. ALLOCATION OF RESPONSIBILITY

4.1. Parties will ensure compliance with applicable privacy laws and regulations.

4.2. The authorized processing operations will be carried out by Processor within an automated environment.

4.3. The Processor shall only be responsible for processing the personal data under this Data Processing Agreement, in accordance with the Controller's instructions and under the (ultimate) responsibility of the Controller. The Processor is explicitly not responsible for other processing of personal data, including but not limited to processing for purposes that are not reported by the Controller to the Processor, and processing by third parties and / or for other purposes.

4.4. Controller represents and warrants that it has express consent and/or a legal basis to process the relevant personal data. Furthermore, the Controller represents and warrants that the contents are not unlawful and do not infringe any rights of a third party. In this context, the Controller indemnifies the Processor of all claims and actions of third parties related to the processing of personal data without express consent and/or legal basis under this Data Processing Agreement.

ARTICLE 5. ENGAGING OF THIRD PARTIES OR SUBCONTRACTORS

5.1. The Processor is authorised within the framework of the Agreement to engage third parties, without the prior approval of the Controller being required. Upon request of the Controller, the Processor shall inform the Controller about the third party/parties engaged.

5.2. The Processor shall in any event ensure that such third parties will be obliged to agree in writing to the same duties that are agreed between the Controller and the Processor.

ARTICLE 6. SECURITY

6.1. The Processor will take care of adequate technical and organisational measures against loss or any form of unlawful processing (such as unauthorised disclosure, deterioration, alteration or disclosure of personal data) in connection with the performance of processing personal data under this Data Processing Agreement.

6.2. The Processor will endeavour to ensure that the security measures are of a reasonable level, having regard to the state of the art, the sensitivity of the personal data and the costs related to the security measures.

6.3. The Controller will only make the personal data available to the Processor if it is assured that the necessary security measures have been taken.

6.4. The Processor has its own responsibility concerning software that is installed by the Controller himself, the processor is never responsible for maintaining, updating and keeping this software safe.

6.5. If Controller uses the PestScan API, he is responsible for the data retrieved with the API. He is also responsible for securing the software that invokes the API and for securing the API calls.

ARTICLE 7. DUTY TO REPORT

7.1. In the event of a security leak and/or the leaking of data, as referred to in the GDPR, the Processor shall, to the best of its ability, notify the Controller thereof with undue delay, after which the Controller shall determine whether or not to inform the Data subjects and/or the relevant regulatory authority(ies). This duty to report applies irrespective of the impact of the leak. The Processor will endeavour that the furnished information is complete, correct and accurate.

7.2. If required by law and/or regulation, the Processor shall cooperate in notifying the relevant authorities and/or Data subjects. The Controller remains the responsible party for any statutory obligations in respect thereof.

7.3. The duty to report includes in any event the duty to report the fact that a leak has occurred, including details regarding:

- the (suspected) cause of the leak;
- the (currently known and/or anticipated) consequences thereof;
- the (proposed) solution;
- the measures that have already been taken.

ARTICLE 8. HANDLING REQUESTS FROM INVOLVED PARTIES

8.1. Where a Data subject submits a request to the Processor to inspect, as stipulated by article 35 GDPR, or to improve, add to, change or protect their personal data, as stipulated by article 36 GDPR, the Processor will forward the request to the Controller and the request will then be dealt with by the Controller. The Processor may notify the Data subject hereof.

ARTICLE 9. NON DISCLOSURE AND CONFIDENTIALITY

9.1. All personal data received by the Processor from the Controller and/or compiled by the Processor within the framework of this Data Processing Agreement is subject to a duty of confidentiality vis-à-vis third parties. Processor shall not use this data for any purpose that was not intended by the Controller, unless the data is modified to such an extent that it cannot be linked to a person or organization.

9.2. This duty of confidentiality will not apply in the event that the Controller has expressly authorised the furnishing of such information to third parties, where the furnishing of the information to third parties is reasonably necessary in view of the nature of the instructions and the implementation of this Data Processing Agreement, or if there is a legal obligation to make the information available to a third party.

ARTICLE 10. AUDIT

10.1. In order to confirm compliance with this Data Processing Agreement, the Controller shall be at liberty to conduct an audit by assigning an independent third party who shall be obliged to observe confidentiality in this regard. Any such audit will follow the Processor’s reasonable security requirements, and will not interfere unreasonably with the Processor’s business activities.

10.2. The audit may only be undertaken when there are specific grounds for suspecting the misuse of personal data, and no earlier than two weeks after the Controller has provided written notice to the Processor.

10.3. The processor shall cooperate with the audit and provide all relevant information reasonably relevant to the audit, including supporting data such as system logs as timely as possible and within a reasonable period of time, whereby a maximum period of two weeks is deemed reasonable, unless an urgent interest opposes this.

10.4. The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented accordingly as the case may be by one of the Parties or jointly by both Parties.

10.5. The costs of the audit will be borne by the Controller.

ARTICLE 11. DURATION AND TERMINATION

11.1. This Data Processing Agreement is entered into for the duration set out in the Agreement, and in the absence thereof, for the duration of the cooperation between the Parties.

11.2. The Data Processing Agreement may not be terminated in the interim.

11.3. This Data Processing Agreement may only be amended by the Parties subject to mutual consent.

11.4. After termination of the Processing Agreement, Processor will destroy the personal data received from the Controller without delay, unless the parties agree otherwise or unless a statutory retention period has to be observed.

11.5. The Processor shall provide its full cooperation in amending and adjusting this Data Processing Agreement in the event of new privacy legislation.

ARTICLE 12. MISCELLANEOUS

12.1. The Data Processing Agreement and the implementation thereof will be governed by Dutch law.

12.2. Any dispute arising between the Parties in connection with and/or arising from this Data Processing Agreement will be referred to the competent Dutch court in the district where the Processor has its registered office.

12.3. In the case of any inconsistency between documents and the appendices thereto, the following order of priority will apply:

1. the Agreement;
2. this Data Processing Agreement;
3. the general Terms and Conditions of the Processor, as can be found on www.pestscan.eu/docs/conditions.html;
4. The Terms and Conditions ICT Office of the Processor, as can be found on www.pestscan.eu/docs/conditions.html;
5. additional conditions, where applicable.

IN WITNESS WHEREOF, the Parties have caused this Data Processing Agreement to be executed by their duly authorized representatives.

Controller	**Processor**
Date:	17 May 2018
Name:	*J. C. Smits*
Signature:	

ANNEX 1 SPECIFICATION OF PERSONAL DATA AND PERSONS CONCERNED

In the context of the Agreement, the Processor will process the following (special) personal data on behalf of the Controller: None.

The Processor will not accept any liability if the Controller processes special personal data, such as religion, sexual preference or medical data. The Processor's software is not intended for recording such data.

The Processor will process the following types of personal data on behalf of the Controller:

- Email addresses
- IP Addresses
- Name, address, city and telephone number
- Financial (bank account number)

It concerns the following categories of stakeholders:

- Staff members
- Customers
- Suppliers

The Controller guarantees that the personal details and categories of data subjects described in this Appendix 1 are complete and correct, and indemnifies the Processor against any defects and claims that result from an incorrect representation by the Controller.

ANNEX 2 SECURITY MEASURES

Processor has taken the following security measures:

- - logical access control, using strong passwords;
- - physical measures for access security;

- - organizational measures for access security;
- - security of network connections via Transport Layer Security (TLS) technology;
- - duty of confidentiality for employees and third parties engaged.
- - Intrusion prevention system (network)
- - Limited access to various levels within the organization and networks
- - Software audits to detect and improve weak spots on time.

SOURCE NOTIFICATION

We wish to thank DHPA for making the template available for this agreement. Formal acknowledgment: "Derived from: DHPA and ICTRecht Processor Agreement Version 01-2016"