PROCESSOR AGREEMENT
MULBERRY GARDEN B.V.

The undersigned:

1. the private limited company {COMPANY NAME}, with registered office and place of business in {ADDRESS}, Chamber of Commerce number: {NUMBER}, and duly legally represented by {NAME}, {JOB TITLE} hereinafter referred to as **Controller**;

and:

2. the private limited company **MULBERRY GARDEN B.V.**, with registered office and place of business in The Hague, Dutch Chamber of Commerce number 66727375 and duly legally represented by – acting on his own – independent authorised Director R.F. Philipse, hereinafter referred to as **Processor**;

take into consideration the following:

- **that** the General Data Protection Regulation (GDPR) shall apply immediately as per 25 May 2018;

- **that** the Controller and Processor have concluded an agreement including the processing of personal data, the reason why the Controller and the Processer are obligated to conclude a so-called Processor Agreement as referred to in Article 28(3) of the GDPR, to rule out that the Processor does not process those personal data for his own purposes;

agree as follows.

Preamble

Wherever in this Processor Agreement terms are used conform definitions from Article 4 of the GDPR, the definitions used in the GDPR shall apply to these terms.

Article 1. Definitions

Without prejudice to the provisions of the GDPR, in this Processor Agreement the terms are defined as:

a. **Main agreement**: the agreement concluded between the Controller and Processor in relation to the Controller's use of the cloud services offered by the Processor, including however not limited to hosted remote desktop and SpinOffice CRM, in this agreement hereinafter referred to as Hosted Services;

b. **Controller**: the legal representative under (1) referred to in this agreement, who defines the objectives of and the resources for the Processing of the Personal Data;

c. **Processor**: the private limited company Mulberry Garden B.V., which is a legal entity that processes Personal Data on behalf of the Controller;

d. **Sub-processor**: a natural or legal person who processes Personal Data by order of the Processor on behalf of the Controller;

e. **GDPR**: the General Data Protection Regulation**,** i.e. the European regulation, on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data within the European Union;

f. **Personal Data**: all information on an identified or identifiable natural person ("the **Stakeholder**"); identifiable is considered a natural person who can directly or indirectly be identified, in particular through a identifier such as a name, an identification number, location details, an online identifier or one or more elements characteristic for the physical, physiological, genetically, psychological, economic, cultural or social identity of that natural person; Personal Data also includes, unless further specified, Particular Personal Data such as Personal Data including race, ethnic origin, political views, religious or philosophical beliefs or membership of a union; furthermore, genetic data, biometric data with regard to the unique identification of a person, information regarding health, details in relation to someone's sexual behaviour or sexual preference (Article 9(1) of the GDPR); personal data related to criminal convictions and criminal offences (Article 10 GDPR); as well as citizen service number (abbreviated as BSN in Dutch);

g. **Customer data**: all (Personal) Data the Controller has recorded using the Hosted Services, and which can be accessed by the Controller via the Internet;

h. **Supervisor**: the Dutch Data Protection Authority (DPA) is the Dutch independent governing body appointed Supervisor by law in the Netherlands to monitor the processing of Personal Data;

i. **File**: every structured group of (Personal) Data accessible according to certain criteria, irrespective of whether this group is centralised or decentralised, or spread based on functional or geographic grounds;

j. **Processing**: any operation or set of operations which is performed on Personal Data or a set of Personal Data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

k. **Recipient**: a natural person or legal person, a government agency, a service or another body, or a third party, to whom/which the Personal Data are disclosed; government authorities that could possible receive Personal Data as part of a particular research in accordance with the Union Law or the Member State Law are not considered Recipients; the Processing of that data by the government authorities is consistent with the data protection rules that apply to the concerning processing purposes;

l. **Data Breach**: the infringement in relation to Personal Data that accidently or on unlawfully leads to the destruction, the loss, the alteration or the unauthorised disclosure or the unauthorised access to transmission, storage or otherwise processed Personal Data;

m. **Stakeholder**: all information on an identified or identifiable natural person to whom the Personal Data applies;

n. **Processor Agreement**: this present Processor Agreement agreed to by the parties.

Article 2. Subject

2.1 Processor processes Personal Data and other Customer Data made available by or via Controller through the Hosted Service exclusively by order of and for purposes of Controller as part of the implementation of the Main Agreement.

2.2 Work to be carried out by the Processor:

- *hosting*, which means, accommodating the Hosted Services in a cloud;
- *make back-ups* and restore if required;
- *application management*, which means, software patching;
- *technical management*, which means, hardware maintenance;
- *database management*, which means, maintenance and patching;
- *helpdesk*, which means, researching and answering questions in relation to the Hosted Services;
- *communication* (such as message traffic);
- *secure destruction* of data carriers.

2.3 Processor shall not process the Personal Data for any other purpose, subject to differing legal requirements.

2.4 Processor undertakes to carefully process Personal Data made available by or via Controller as part of the abovementioned operations.

Article 3. Effective date and duration

3.1 This Processor Agreement is effective at the time of signing and continues for as long as the Processor operates as Processor of Personal Data of the Personal Data made available by the Controller.

3.2 The Processor Agreement ends when every File owned by the Controller has been destroyed by the Processor.

3.3 Obligations that are by their nature intended to continue after termination of this Processor Agreement, shall continue to apply. These obligations include, in any event, the provisions with regard to confidentiality, liability and applicable law.

3.4 Processor does not retain the Personal Data longer than the agreed to retention period, however in any case no longer than 3 months after termination of the Main Agreement on the basis of which the data is processed.

Article 4. Termination of the agreement

4.1 Upon termination of the agreement and if required by the Controller, the Processor shall ensure that a back-up of the Personal Data in the Processor's system can be supplied to the Controller or a third party selected by him. Costs incurred as a result of providing the back-up are at the expense of the Controller. This data is not encrypted, unless Controller decides otherwise. Needless to say, in that case a key exchange shall take place.

4.2 Processor destroys all Personal Data and shall at the very least honour the Controller's basic instructions.

4.3 Processor shall at all times adhere to the above mentioned right to transferability of data in accordance with Article 20 of the GDPR in such a manner that there is no loss of functionality or (parts of) the data.

Article 5. Processor's obligations, general

5.1 Commissioned by or for the benefit of Controller, Processor shall process Personal Data for the purpose of the agreement and objective as further specified in the Main Agreement. Other Processing shall exclusively be carried out as a supplementary commission and in accordance with written instructions issued by Controller or, if subject to, a statutory obligation to that effect.

5.2 Processor has no authority over the Personal Data supplied. He does not make decisions regarding receipt and use of the data, disclosure to third parties nor the duration of the storage period of the data. Authority over the Personal Data, administered by the Controller to the Processor under this Processor Agreement, shall under no circumstances be vested with the Processor.

5.3 Upon intermediate request from the Controller, Processor shall make the Personal Data as they are saved in the Processor's system (under management of the Processor) available within 4 weeks pertaining to this Processor Agreement. Costs incurred as a result of these endeavours by Processor are at the expense of the Controller insofar these costs have not explicitly been included to the agreed to fees and reimbursements under the Main Agreement.

5.4 Processor shall provide Controller with all the requested information if a Stakeholder makes us of their rights based on the GDPR. The Processor will immediately provide an answer in writing in understandable terms, and may not impose extra costs therefore.

5.5 Processor enables the Controller at all times to adhere to the obligations within the statutory time-limits based on the GDPR, particularly concerning the rights of the Stakeholder(s), such as but not limited to an access authorisation request, improvement, supplement, deletion or blocking of Personal Data and dealing with an objection that has been submitted and accepted.

5.6 Processor shall process the Personal Data from Controller separately from Personal Data he processes for himself or on behalf of a third party.

Article 6. Hailing Data Breaches

6.1 Without unreasonable delay and no later than 24 hours after discovery, the Processor shall notify the Controller of a Data Breach via email to the Controller's contact person.
Processor includes the following in the email:
- name of the Processor and contact person;
- telephone number;
- substance of the infringement or the Data Breach;
- size of File of the Data Breach;
- if the data is/has been made accessible to unauthorised persons;
- day and time when infringement or Data Breach was observed.

6.2 Processor is prohibited to report a Data Breach to the Dutch Data Protection Authority on behalf of the Controller.

6.3 Processor is committed to cooperate with the Controller to meet all the legal requirements in relation to the reporting to the Dutch Data Protection Authority. Specifically, Processor must fulfil the following requirements in case of a Data Breach:

a. Processor submits (insofar he is in the possession thereof) the required information to the Controller for the Data Breach assessment;
b. Processor shall keep the Controller informed of the progress of the internal investigation and the developments with regard to the Data Breach;
c. Processor renders his/her assistance in the Data Breach investigation;
d. Processor keeps the Controller informed on the recently implemented security measures adopted to minimise the Data Breach and to prevent it from happening again;
e. Processor renders his/her assistance so the Controller is capable of notifying the Stakeholder(s).
f. Processor follows the reasonable instructions from the Controller in relation to the coordination of the events of the Data Breach; and
g. Processor conforms to the binding Dutch Data Protection Authority requirements, even if these are appointed to the Controller, provided that the guidelines concern the Processor's own work.

Article 7. Duty of confidentiality

7.1 Processor, as well as people employed by the Processor or engaged in work on behalf of the Processor, are obligated to keep Personal Data they could take a note of as a result of this Processor Agreement confidential, unless a mandatory statutory provision or court decision requires disclosure or disclosure is necessary in the context of the performance of the Processor Agreement. Processor ensures that any person acting under his/her authority is obligated to keep Personal Data he/she is made aware confidential. A confidentiality agreement is signed by this person to ensure this.

7.2 If the Processor receives a request, an order or an injunction from a Dutch or foreign Supervisor, government agency or an investigatory, criminal or national security authority to give (access to) Personal Data, the Processor shall immediately notify the Controller thereof. When dealing with the request or injunction, the Processor honours all the Controller's instructions (including instruction to leave the processing of the request or injunction entirely or partially over to Controller) and renders all reasonably necessary cooperation to the Controller.

7.3 If the Processor is prohibited by law from complying with its obligations on the basis of the request, the order or the injunction as mentioned in the clause above, the Processor shall promote the Controller's reasonable interests.
Processor shall in that case:

- procure a legal assessment of the extent to which (i) the Processor is required by law to comply with the request, the order or the injunction; and (ii) the Processor is in fact prohibited from complying with its obligations to the Controller based on the abovementioned clause;
- only cooperate with the request, the order or the injunction if the Processor is required by law to do so, and the Processor shall object where possible (by legal action) to the request, order or injunction against informing the Controller in this respect or against following the Controller's instructions.
- not provide any more Personal Data than strictly necessary to comply with the request, the order or the injunction.

Article 8. Security measures

8.1 The Processor shall take appropriate technical and organisational measures to safeguard a level of security attuned to the risk. These measures shall adapt to the changes and developments of the market.
They should include the following:
a. measures to guarantee the confidentiality, the availability and the integrity and resilience of the processing systems in the event of a physical or technical (security) incident;
b. measures to immediately recover the availability of and the accessibility to the Personal Data in the event of a physical or technical (security) incident;
c. measure to ensure that only authorised persons have access to the Personal Data;
d. measures to identify the weak areas with respect to the Processing of the Personal Data in the systems used by the Processor and by third parties hired by the Processor for the provision of services to Controller; and
e. a procedure to test, assess and evaluate on set times the effectiveness of the security measures.

8.2 The Controller is entitled to have the Processing of the Personal Data perform an audit by an independent external expert. Processor gives Controller the opportunity, if Controller so requests, to perform a periodic audit at least once a year at a date and time and scope of the investigation to be determined by the parties. The external costs of the audit as well as costs incurred by Processor as a result of this audit are at the expense of the Controller.

8.3 In addition to clause 3 of this Article, the Controller has the right to inspect the Processing of the Personal Data more than once a year on a date and time and scope of the investigation to be determined by the parties as referred to above, if and insofar Controller has a verifiable well-founded suspicion that the Processor does not fulfil his requirements under the Processor Agreement. The costs of this audit as well as costs incurred by Processor as a result of this audit are at the expense of the Controller. Controller shall ensure that the investigation is carried out in such a way that Processor does not experience any or as little as possible inconvenience as a result thereof. Controller shall submit a complete and an unaltered copy of the research findings to the Processor as soon as possible.

8.6 Processor undertakes to provide the Controller, or the commissioned auditor, with the requested information within a time period set by the Controller. With this, the Controller, or the commissioned auditor, can form an opinion about the adherence by the Processor to this Processor Agreement. The Controller, or the commissioned auditor, are bound to observe confidentiality in respect of all information regarding these inspections.

8.7 Controller and Processer shall consult each other after the investigation to see if and to what extent adjustments to the organisational and security measures are necessary to meet the mandatory legislation from the GDPR in effect at that time.

8.8 Processor ensures the appropriate measures for all risks as a result of destruction, loss, amendments, unauthorised disclosure of, unauthorised access to, transmission, storage, or in any other way processed Personal Data, albeit accidentally, or unlawfully has been minimised to an acceptable level for the Controller.

Article 9. Engagement of third parties (Sub-processor)

9.1 Following the assignment and objective, as further specified in the Main Agreement, Processor is entitled to use services of a Sub-processor within the European Union. If the Sub-processor is located in a country outside of the European Union, this shall take place only after explicit permission has been granted by the Controller, which permission shall not be withheld on unreasonable grounds.

Processor shall at Controller's first request inform of the identity and registered location of the Sub-processor.

9.2 Work the Sub-processor could be asked to carry out include:
- hosting, which means, harbouring the Hosted Services in the cloud, by facilitating a secured area for the Processor's servers that are permanently connected to the Internet;
- making back-ups and restore if required;
- technical management, which means, hardware maintenance; and
- safely destroying data carriers.

9.3 Processor shall impose obligations on the Sub-processor the Processor employed which are equivalent to the obligations from this Processor Agreement Processor has to adhere. The Processor shall in these circumstances at all times be the contact person and person responsible to ensure compliance with the provisions of this Processor Agreement and shall allow the Controller, if so requested by them, to examine the agreement made with this Sub-processor where these obligations have been incorporated.

Article 10. Changes to the Processor Agreement

10.1 Controller and Processor shall coordinate with each other about proposed changes to the Processor Agreement, if a regulation amendment or an amendment to the explanation of the regulation gives grounds to do so.

10.2 Amendment to this Processor Agreement can only take place in writing.

Article 11. Liability

11.1 Processor is held liable pursuant to Article 82 of the GDPR for all damage or loss by failure to comply with the Processor Agreement, including when the Processor does not meet the obligations of the GDPR specifically related to processing, or has acted outside of the lawful instructions of the Processor Agreement.

11.2 Processor indemnifies Controller against all damages or loss insofar this has been caused by the work done by the Processor.

Article 12. Applicable law

12.1 The Processor Agreement and its performance are governed by the laws of the Netherlands.

12.2 All disputes arising in connection with the Processor Agreement shall be submitted to the competent court as stipulated in the Main Agreement.

Article 13. Reference title

13.1 This agreement may be cited as Processor Agreement Mulberry Garden.

Thus agreed on, drawn up in duplicate and signed:

City:	**.....**	**The Hague**
Date:	**.....**	**..... 2023**

{Company Name}	**Mulberry Garden B.V.**
{Name of Director}	**R.F. Philipse**