Data Processing Agreement

Data Controller, being the signed customer (hereafter: Controller) and **Data Processor: Make it WorkPress** and any of her other brandnames, establed at the Potgieterlaan 6, Zeist, registered under KVK54845874 and represented by Michiel Tramper (hereafter: Processor), hereafter called Parties and individually Party, have concluded this Data Processing Agreement (DPA) concerning the processing of personal data by the Processor on behalf of the Controller and have agreed as following:

1: Definitions

In this Data Processing Agreement, capitalized terms shall have the meaning set forth in this Article. Where the definition in this article is included in the singular, the plural is also included and vice versa, unless explicitly stated otherwise or if the context dictates otherwise.

1.1 GDPR: the Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.2 Data Subject: the identified or identifiable natural person to whom the Personal Data relate.

1.3 Appendix: an appendix to this Data Processing Agreement, which forms an integral part of this Data Processing Agreement.

1.4 Special Categories of Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the unique identification of a person, or data concerning health, or data concerning a person's sexual conduct or sexual orientation.

1.5 Third Party: a natural person or legal entity, a government agency, a department or another body, not being the Data Subject, neither the Controller, nor the Processor, nor the persons authorised to process Personal Data under the direct authority of the Controlelr or the Processor.

1.6 Service: the service(s) to be provided by the Processor to the Controller on the basis of the Agreement.

1.7 Infringement in connection with Personal Data: a breach or suspicion of a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data that has been transmitted, stored or otherwise processed**.**

1.8 Employee: the employees engaged by Processor and other persons whose work falls under his responsibility and who are engaged by Processor for the performance of the Agreement.

1.9 Receiver: a natural or legal person, a public authority, a department or another body, whether or not a Third Party, to whom or to which the Personal Data are provided.

2. Purpose of the processing

2.1 This agreement has been entered into with respect to the use of the Processor's services by the Controller as part of the subscription and additional services. The processing relates to one or more services as described in Appendix 1 and will only take place for one or more purposes as described in Appendix 2.

2.2 The Data Processing Agreement supplements the Agreement and replaces any agreements made previously between the Parties with regard to the Processing of Personal Data.

2.2 The provisions of the Data Processing Agreement shall apply to all Processing Operations that take place pursuant to the Agreement. Processor shall immediately inform the Controller if Processor has reason to believe that Processor can no longer comply with the Data Processing Agreement.

2.3 The Controller shall issue instructions and instructions to the Processor to process the Personal Data on behalf of the Controller. The instructions of the Processing Agent are described in detail by the Controller. The Controller may reasonably issue additional or different instructions in writing. However, the Agreement and the Main Agreement are interdependent and cannot be terminated separately

2.4 The Processor shall process the Personal Data exclusively on the instructions of the Controller and on the basis of the instructions of the Controller. Processor shall only process Personal Data insofar as the Processing is necessary for the performance of the Agreement, never for its own benefit, for the benefit of Third Parties and/or for advertising purposes or other purposes, unless a provision of EU or national law applicable to the Processor requires Processor to process the personal data. In such a case, Processor shall notify the Controller of this provision in writing prior to the Processing, unless such legislation prohibits such notification for important reasons of public interest.

2.5 The processor shall process the types of personal data and the category of Data Subjects set out in Appendix 3. The personal data to be processed shall remain the property of the Controller and/or the data subjects concerned.

3. Processor Obligations

3.1 The Processor shall ensure compliance with the conditions legally imposed when processing personal data for the controller on the basis of the instructions of the controller.

3.2. The Processor shall ensure that all necessary technical, organisational and other additional measures are taken to ensure that the personal data are not inadvertently made public or unlawfully processed. The obligations that arise for the Processor from this Data Processing Agreement also apply to the party that processes personal data on the instructions of or under the authority of the Processor. The security measures taken by the Processor are described in Appendix 4.

3.3 The Processor shall cooperate with the Controller where consultation of the processing is necessary, such as prior to the consultation of a supervisor or in the context of a data protection impact assessment. The Processor may reasonably charge the Controller for this.

3.4. Although the processor ensures that appropriate security measures are taken, the processor cannot guarantee that the security is effective in any case. In the event of a threat or failure of the security measures, the processor shall do as much as reasonably possible to limit the loss or disclosure of personal data as much as possible.

3.5. In the event of the discovery or suspicion of an Infringement in connection with Personal Data leading to a significant risk with serious adverse consequences or actual serious consequences, the processor shall inform the controller within 48 hours of its discovery. In the light of the controller's assessment, the Personal Data Authority and the Data Subjects may be informed, if there is a legitimate desire to do so. If legislation requires this, the Processor will cooperate in informing the authorities and/or parties involved that are relevant to the infringement.

3.6. In the event of an actual Infringement in connection with Personal Data, the Processor shall report the data breach, the alleged cause of the breach, the expected consequences, the proposed solution and/or measures already taken, the contact details for the follow-up, the maximum number of Data Subjects from whom data have been leaked and the description of this group of Data Subjects, the type of personal data leaked, the date or period on which the breach occurred, the date on which the breach was discovered by the processor, and whether the personal data leaked have been encrypted or otherwise made inaccessible to unauthorised persons.

4. Controller Obligations

4.1 The Controller shall ensure that the processing of personal data submitted by the Controller is carried out for legitimate purposes. The Controller shall thereby guarantee that the Processor does not process more data than necessary for the legitimate purposes specified.

4.2 The Controller shall be responsible for ensuring a legitimate and legally valid basis for the processing of data, including at the time of transfer of personal data to the Processor. The Processor shall have the right to ask for the written documentation for this basis.

4.3. The Controller shall assure the Processor that the Data Subjects and/or Data Subjects to which the personal data are owned have received adequate information about the processing of their personal data..

4.4. If the Controller itself employs a sub-processor in relation to the contract, the Processor must be informed immediately.

4.5. The Controller shall be responsible for arranging appropriate technical and organisational security measures in respect of used software, plug-ins and applications within the services provided by the Processor.

4.6 The Controller shall make public the contact details of any contact in the field of privacy to the Processor. The Processor shall not be responsible for any damage caused by the provision of incorrect contact details by the Controller.

4.7. The Controller shall ensure that instructions given by the controller in relation to the agreement do not conflict with the GDPR or data protection provisions of any EU Member State and are therefore in compliance with privacy legislation.

4.8. The Controller shall only make personal data available to the Processor if the Controller is satisfied that appropriate security measures have been put in place.

4.9 The Controller shall ensure that it complies with any statutory reporting requirements.

5. Transfer of Data

5.1 The Processor may, in countries within the European Union, process personal data. If the legal requirements are met, the Processor may also process personal data in countries outside the European Union.

5.2 The Processor shall only transfer personal data to recipients in the United States if companies comply with the requirements set out on the basis of the EU/US Privacy Shield or the model agreements made available by the EU/EUR.

6. Processing by sub-processors or Third Parties

6.1 Pursuant to this processing agreement, the Processor may involve sub-processors in the processing of personal data, with due observance of the applicable privacy legislation. The Processor shall not engage any other processor for the performance of the Contract other than with the specific written consent of the Controller.

6.2 The Controller hereby authorizes the processor to enter into contracts with sub-processors. The Processor shall inform the Controller of any changes concerning the addition or replacement of sub-processors and/or third parties. The sub-processors concerned by the Agreement are listed in Appendix 5.

6.3 In the event of an agreement with a sub-processor, the Processor shall enter into processing agreements with EU/EEA sub-processors. Outside the EU/EEA, the Processor will come to an agreement in accordance with the standard contractual clauses for the transfer of personal data to processors in third countries or in accordance with the EU/US Privacy Shield.

6.3 The Controller shall have the right to object to any newly introduced sub-processor in writing, stating the reasons, within 14 days of the announcement, after which the two Parties shall attempt to reach a joint solution.

6.4 The Processor shall ensure that the sub-processors assume the same obligations as those agreed between the Controller and the Processor, with the Controller having the right to inspect the relevant agreements. The Processor shall ensure that these obligations are properly complied with and shall be reasonably liable to the Controller in the event of errors on the part of sub-processors.

7. Rights of Data Subjects

7.1 If a Data Subject makes use of his or her legal right with regard to his or her personal data and contacts the Processor to this end, the Processor shall pass on this request to the Controller. In such a case, the Controller shall assume responsibility for further processing of that request, with the Processor having the right to inform the data subject thereof. The Processor shall ensure that sub-processors do not respond to requests unintentionally or independently, unless written instructions or permission has been granted for this.

7.2. In the case of a Data Subject's request with regard to his or her personal data, the Processor shall provide reasonable technical assistance to execute the request, if the Controller so requests. The Processor shall be entitled to charge the Controller reasonable costs for this.

8. Audit

8.1 The Controller has the right to have an audit carried out by an independent third party, which has been agreed by both the undersigned Parties if the Controller believes that the Data Processing Agreement is not being sufficiently complied with.

8.2. The audit shall only take place in the event of a concrete and written suspicion of inadequate enforcement of the Processor's contract and/or misuse and errors in the processing of personal data by the Processor. The audit shall take place 14 calendar days after the written announcement by the Controller.

8.3 The Processor shall cooperate in supplying all necessary and relevant information within a reasonable period of a maximum of 14 days. The costs of the audit shall be borne by the Controller.

8.4 The results of the audit will be assessed by the undersigned Parties in mutual consultation and whether or not they will be implemented jointly.

9. Secrecy

9.1 The Processor shall ensure that all personal data of the Data Subjects received by the Processor via the Controller is kept confidential from third parties. The Processor shall also ensure that Employees employed by the Processor shall comply with the confidentiality obligation as described in this article, and shall limit this to those Employees for whom access is necessary on the basis of their tasks.

9.2. If any Party has given its written consent to the provision of information to third parties and the provision of such information is necessary in view of the nature of the Agreement and the performance of this Processing Agreement, the obligation of confidentiality towards Third Parties shall not apply

9.3 The obligation to maintain confidentiality does not apply if public disclosure of personal data is required on legal grounds or on the basis of a judicial decision. If this is the case, the Processor shall report this to the Controller.

10. Liability

10.1 The compensation for damage that falls to the Processor's liability as a result of a shortcoming attributable in the follow-up to the Data Processing Agreement shall be limited per event, whereby a series of successive events shall be regarded as one event, to a maximum of the amount of the compensation received by the Processor in the month prior to the event in which the damage was caused.

11.2 In the case of culpable damage, the Processor shall only be responsible for direct damage, including only the following cases: direct damage to material goods; the so-called material damage; reasonable and demonstrable costs for the Processor to comply with the Data Processing Agreement; reasonable costs for determining the direct damage; and reasonable but demonstrable costs incurred by the Processor to prevent or limit direct damage as described in this article.

11.3 The Processor is not liable for any indirect damage, i.e. all damage that is not direct damage. This shall in any event include, but not be limited to, consequential damages, lost profits, lost savings, damages due to business interruption, reduced goodwill, damages caused by the use of data or data prescribed by the Controller, or the loss, destruction or corruption of data.

11.4 If a Controller claims damages, these must be explicitly and specifically reported. If this is not the case, this claim expires after the expiry of 12 months.

11.5 The Processor shall only be liable for an attributable failure to comply with the Data Processing Agreement if the Controller gives the Processor written notice of default within 48 hours and the Processor does not remedy this within a reasonable period of time. The Processor shall thereby have the right, after notification, to resolve the shortcoming within a reasonable period of time. The notice of default must be drawn up as accurately and completely as possible, so that the Processor is in a position to resolve this properly.

11. Duration and Discontinuation

11.1 This Data Processing Agreement shall enter into force upon signature by both Parties.

11.2 This Data Processing Agreement is entered into for the period during which the Processor processes personal data on the instructions of the Controller.

11.3 If the Agreement is terminated, this Data Processing Agreement shall also terminate. Both parties have the right to terminate the Agreement, taking into account the notice period of 1 month.

11.4 After the termination of the Agreement or Data Processing Agreement, the Processor shall remove and destroy the personal data it contains within 30 days, unless legislation requires that these data be retained. As long as the Processor continues to process personal data, the obligations as set out in this Data Processing Agreement shall continue to apply.

11.5 Upon termination of the agreement, the Processing Officer is himself/herself/responsible for the transfer and/or export of his/her personal data.

12. Applicable Law

12.1 In the event of any conflict between the provisions of the Data Processing Agreement and the Agreement, the provisions of the Data Processing Agreement shall prevail.

12.2 This Data Processing Agreement and the performance of this Data Processing Agreement shall be governed by Dutch law.

12.3 If any disputes or conflicts arise with respect to this agreement, they shall be submitted to the competent court in the district of the Processor.

In witness whereof, the Parties through their duly authorized representatives hereby agree to the terms of this Data Processing Agreement.

Data controller:	**Data processor:**
Company Name:	Company Name: CreativeSolvers
Name:	Name: Michiel Tramper
Title:	Title: Owner
Address:	Address:
	Potgieterlaan 6, 3702 GS Zeist,
	Netherlands
Chamber of Commerce or Company registration number (if applicable):	Chamber of Commerce or Company registration number (if applicable):
	KVK54845874
Signature:	Signature:

Appendices

Appendix 1: Services in Processing Personal Data

The Processor processes personal data for the following services:

- Managed WordPress Hosting and
- Web Hosting
- E-mail
- Domain name registration
- Website Transfer
- Content Management
- Content Delivery Network

The Controller confirms that the data listed in Appendix 1 are correct and indemnifies the Processor against any defects or liability due to an incorrect presentation by the Controller.

Appendix 2: Objectives for Processing Personal Data

The Processor processes personal data for the following purposes:

- Hosting
- Security
- Domain Registration
- Invoicing
- Support on Services

The Controller confirms that the data listed in Appendix 2 are correct and indemnifies the Processor against any defects or liability due to an incorrect presentation by the Controller.

Appendix 3: Species and Categories of Processed Personal Data

The Processor shall process the following categories of personal data names of the Processor:

- Contact details
- Name, Address and Place of residence details
- Language, Country and Time Zone
- Information about products ordered
- E-mails, submissions of contact forms or chat messages and other communications
- Customer number if applicable
- Payment details if applicable
- Login data if applicable
- IP address
- Other data stored through the processor's services

The following categories are involved in the processing:

- Customers
- Potential customers
- Website visitors
- Website users
- Suppliers
- Account holders
- Employees
- Persons in the other category whose personal data are processed by the services provided by the Processor.

The Controller confirms that the data listed in Appendix 3 are correct and indemnifies the Processor against any defects or liability due to an incorrect presentation by the Controller.

Appendix 4: Security measures relating to the Processing of Personal Data

The Processor has taken technical and organizational measures to secure the processing of personal data:

- Two-factor authentication and use of strong passwords for server management
- Use of secure connections where possible
- Encryption of backup files
- Encryption of corporate computer disks
- Centralized password management
- Encrypted storage of passwords and optionally other personal data
- Collaboration with adequate suppliers with the highest possible level of security measures.
- Target access restrictions on different levels of users
- Monitoring of the applications used by the Controller
- Periodic updating of software and applications

Appendix 5: Subprocessors

Subprocessor	Personal data processed	Country of Processing	Country of residence Subprocessor
Cloudways	Other data stored by the Processor. E-mails, entries of contact forms and other communications, IP Address,	Depending on the server location chosen by the Processing Officer. In most cases the Netherlands.	Malta

Mailgun	E-mails, contact form submissions and other communications, IP Address, e-mail address, Name	EU	United States
WordFence	IP Address, Other data stored by the Processor	United States	United States
Transip	Name, address and locality data, e-mail address, telephone number, company name	The Netherlands	The Netherlands
Cloudflare	Other data stored by the Processor	United States	United States
ManageWP	Other data stored by the Processor	United States/EU	United States

The Controller agrees that the Processor shall use the above sub-processors to provide the agreed services to the Controller. In the case of maintenance only subscriptions, only WordFence and ManageWP are utilized as a subprocessor.