DEFIANT

DATA PROCESSING AGREEMENT

The Customer agreeing to these terms ("**Customer**") and **Defiant, Inc.**, having its principal place of business at 800 5th Ave Ste 4100, Seattle, WA 98104 (the "**Processor**") have entered into an agreement for the provision of Services (as amended from time to time; the "**Agreement**").

Each, the Customer and the Processor, may also be referred to as "**Party**" or together referred to as "**Parties**" in this Data Processing Agreement.

This Data Processing Agreement, including its appendices (the "**Data Processing Agreement**") will, as from the Agreement Effective Date (as defined below), be effective and replace any previously applicable data processing agreement or any terms previously applicable to privacy, data processing and/or data security existing between the Parties.

1. **Introduction**.

This Data Processing Agreement reflects the parties' agreement with respect to the terms governing the processing and security of Customer Data under the Agreement.

2. **Definitions**.

2.1. Capitalized terms used but not defined in this Data Processing Agreement have the meanings given elsewhere in the Agreement. In this Data Processing Agreement, unless stated otherwise:

"**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

"**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a party's liability is capped under the Agreement, either per annual period or event giving rise to liability, as applicable.

"**Alternative Transfer Solution**" means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).

"**Agreement Effective Date**" means, as applicable:

25 May 2018, if Customer accepted or the parties otherwise agreed to this Data Processing Agreement in respect of the Agreement prior to or on such date; or

the date on which Customer accepted or the parties otherwise agreed to this Data Processing Agreement in respect of the Agreement, if such date is after 25 May 2018.

"**Audited Services**" means the Services (as defined below).

"**Customer Data**" means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

"**Customer Personal Data**" means personal data contained within the Customer Data.

"**Data Incident**" means a breach of Processor's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems

managed by or otherwise controlled by Processor. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**EEA**" means the European Economic Area.

"End Users" means the users of Customer's website, WordPress platform, or other applications that use the Services or on which the Services are installed.

"**European Data Protection Legislation**" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Full Activation Date**" means: (a) if this Data Processing Agreement is incorporated into the Agreement by reference, the Agreement Effective Date; or (b) if the parties otherwise agreed to this Data Processing Agreement, the eighth day after the Agreement Effective Date.

"**GDPR**" means 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, and repealing Directive 95/46/EC.

"**Processor's Third Party Auditor**" means a Processor-appointed, qualified and independent third party auditor, whose then-current identity Processor will disclose to Customer.

"**Model Contract Clauses**" or "MCCs" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

"**Non-European Data Protection Legislation**" means data protection or privacy legislation other than the European Data Protection Legislation.

"**Notification Email Address**" means the email address(es) designated by Customer to receive certain notifications from Processor.

"**Security Measures**" has the meaning given in Section 7.1.1 (Processor's Security Measures).

"**Services**" means the following services, as applicable: hosted software applications, software products, and related support services.

"Processor's Systems" means the computing and storage infrastructure contracted by Processor to run the Services and to store the Customer Data. For avoidance of doubt, Processor's Systems do not include Google Drive or any other part of Google G Suite used by Customer and contracted by Customer, nor any of the Third Party Offerings.

"**Subprocessors**" means third parties authorized under this Data Processing Agreement to have logical access to and process Customer Data in order to provide parts of the Services and related technical support.

"**Term**" means the period from the Agreement Effective Date until the end of Processor's provision of the Services under the Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Processor may continue providing the Services for transitional purposes.

2.2. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this Data Processing Agreement have the meanings given in the GDPR, and the terms "data importer" and "data exporter" have the meanings given in the Model Contract Clauses, in each case

irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies.

3. **Duration of Data Processing Agreement**. This Data Processing Agreement will take effect on the Agreement Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by Processor as described in this Data Processing Agreement.

4. **Scope of Data Protection Legislation**.

4.1 Application of European Legislation. The parties acknowledge and agree that the European Data Protection Legislation will apply to the processing of Customer Personal Data if:

(a) the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA; and/or

(b) the Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behaviour in the EEA.

4.2 Application of Non-European Legislation. The parties acknowledge and agree that Non-European Data Protection Legislation may also apply to the processing of Customer Personal Data.

5. **Processing of Data**.

5.1 **Roles and Regulatory Compliance; Authorization**.

5.1.1. Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

(a) the subject matter and details of the processing are described in Appendix 1;

(b) Processor is a processor of that Customer Personal Data under the European Data Protection Legislation;

(c) Customer is a controller or processor, as applicable, of that Customer Personal Data under the European Data Protection Legislation; and

(d) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.1.2. Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Processor that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Processor as another processor, have been authorized by the relevant controller.

5.1.3. Responsibilities under Non-European Legislation. If Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.

5.2 **Scope of Processing**.

5.2.1 Customer's Instructions. By entering into this Data Processing Agreement, Customer instructs Processor to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and related technical support; (b) as further specified via Customer's use of the Services and related technical support; (c) as documented in the form of the Agreement, including this Data Processing Agreement; and (d) as further documented in any other written instructions given by Customer and acknowledged by Processor as constituting instructions for purposes of this Data Processing Agreement.

5.2.2 Processor's Compliance with Instructions. As from the Full Activation Date, Processor will comply with the instructions described in Section 5.2.1 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Processor is subject requires other processing of Customer Personal Data by Processor, in which case Processor will inform Customer (unless that law prohibits Processor from doing so on important grounds of public interest) via the Notification Email Address.

6. **Data Deletion**.

6.1. **Deletion During Term**. Processor will enable Customer and/or End Users to delete Customer Data during the Term in a manner consistent with the functionality of the Services. Processor will comply with the instruction to delete data as soon as reasonably practicable, unless EU or EU Member State law requires storage.

6.2. **Deletion on Term Expiry**. Subject to Section 6.3 (Deferred Deletion Instruction), on expiry of the Term Customer instructs Processor to delete all Customer Data (including existing copies) from Processor's Systems in accordance with applicable law. Processor will comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless EU or EU Member State law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the Term expires, any Customer Data it wishes to retain afterwards.

6.3. **Deferred Deletion Instruction**. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Deletion on Term Expiry) is also processed, when the Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Data Processing Agreement will continue to apply to such Customer Data until its deletion by Processor.

7. **Data Security**.

7.1. **Processor's Security Measures, Controls and Assistance**.

7.1.1. Processor's Security Measures. Processor will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). As described in Appendix 2, the Security Measures include measures to help ensure ongoing confidentiality, integrity, availability and resilience of Processor's Systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Processor may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

7.1.2. Security Compliance by Processor Staff. Processor will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3. Processor's Security Assistance. Customer agrees that Processor will (taking into account the nature of the processing of Customer Personal Data and the information available to Processor) assist Customer in ensuring compliance with Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Processor's Security Measures);

(b) complying with the terms of Section 7.2 (Data Incidents).

7.2. **Data Incidents**.

7.2.1. Incident Notification. If Processor becomes aware of a Data Incident, Processor will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2. Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Processor recommends Customer take to address the Data Incident.

7.2.3. Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Processor's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

7.2.4. No Assessment of Customer Data by Processor. Processor will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

7.2.5. No Acknowledgment of Fault by Processor. Processor's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Data Incident.

7.3. **Customer's Security Responsibilities and Assessment**.

7.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Processor's obligations under Section 7.1 (Processor's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):

(a) Customer is solely responsible for its use of the Services, including:

(i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Data;

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and

(iii) backing up its Customer Data; and

(b) Processor has no obligation to protect Customer Data that Customer elects to store or transfer outside of Processor's and its Subprocessors' systems.

7.3.2. Customer's Security Assessment.

(a) Customer is solely responsible for evaluating for itself whether the Services, the Security Measures and Processor's commitments under this Section 7 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable.

(b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Processor as set out in Section 7.1.1 (Processor's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4. **Audits of Compliance**.

7.4.1. Customer's Audit Rights.

(a) If the European Data Protection Legislation applies to the processing of Customer Personal Data, Processor will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Processor's compliance with its obligations under this Data Processing Agreement. Processor will contribute to such audits as described in Section 7.4 (Audits of Compliance).

(b) If Customer decides to conduct an audit as described above, then Customer shall bear all costs and expenses connected therewith, such as the auditors' fees, costs of transport, legal fees etc.

(c) If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Processor will, without prejudice to any audit rights of a supervisory authority under such Model Contract Clauses, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses.

(c) Customer may also conduct an audit to verify Processor's compliance with its obligations under this Data Processing Agreement.

7.4.2. No Modification of MCCs. Nothing in this Section 7.4 (Audits of Compliance) varies or modifies any rights or obligations of Customer or Processor LLC under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA).

8. **Impact Assessments and Consultations**. Customer agrees that Processor will (taking into account the nature of the processing and the information available to Processor) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR.

9. **Data Subject Rights; Data Export**.

9.1. **Access; Rectification; Restricted Processing; Portability**. During the Term, Processor will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict processing of, delete, and to export Customer Data.

9.2. **Data Subject Requests**.

9.2.1. Customer's Responsibility for Requests. During the Term, if Processor receives any request from a data subject in relation to Customer Personal Data, Processor will advise the data subject to submit

his/her request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2. Processor's Data Subject Request Assistance. Customer agrees that (taking into account the nature of the processing of Customer Personal Data) Processor will assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Customer's Responsibility for Requests).

10. **Data Transfers**.

10.1. **Data Storage and Processing Facilities**. Customer agrees that Processor may, subject to Section 10.2 (Transfers of Data Out of the EEA), store and process Customer Data in the United States and any other country in which Processor or any of its Subprocessors maintains facilities.

10.2. **Transfers of Data Out of the EEA**.

10.2.1. Processor's Transfer Obligations. If the storage and/or processing of Customer Personal Data (as set out in Section 10.1 (Data Storage and Processing Facilities)) involves transfers of Customer Personal Data out of the EEA and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), Processor will:

(a) if requested to do so by Customer, ensure that Processor as the data importer of the Transferred Personal Data enters into Model Contract Clauses with Customer as the data exporter of such data, and that the transfers are made in accordance with such Model Contract Clauses; and/or

(b) offer an Alternative Transfer Solution, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available to Customer about such Alternative Transfer Solution.

10.2.2 Customer's Transfer Obligations. In respect of Transferred Personal Data, Customer agrees that:

(a) if under the European Data Protection Legislation Processor reasonably requires Customer to enter into Model Contract Clauses in respect of such transfers, Customer will do so; and

(b) if under the European Data Protection Legislation Processor reasonably requires Customer to use an Alternative Transfer Solution offered by Processor, and reasonably requests that Customer take any action (which may include execution of documents) strictly required to give full effect to such solution, Customer will do so.

10.3. **Data Center Information**. Processor uses Amazon's AWS to host the Service. Information about the locations of Processor data centers is available at: https://aws.amazon.com/about-aws/global-infrastructure/ (as may be updated by Amazon from time to time).

10.4 **Disclosure of Confidential Information Containing Personal Data**. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Processor will, notwithstanding any term to the contrary in the Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11. **Subprocessors**.

11.1. **Consent to Subprocessor Engagement**. Customer specifically authorizes the engagement of Processor's Affiliates as Subprocessors. In addition, Customer generally authorizes the engagement of any other third parties as Subprocessors ("**Third Party Subprocessors**"). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Processor LLC of the processing of Customer Data if such consent is required under the Model Contract Clauses.

11.2. **Information about Subprocessors**. Information about Subprocessors is available in Appendix 3 and may be updated by Processor from time to time in accordance with this Data Processing Agreement).

11.3. **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Processor will:

(a) ensure via a written contract that:

(i) the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this Data Processing Agreement) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Processor as described in Section 10.2 (Transfers of Data Out of the EEA); and

(ii) if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Data Processing Agreement, are imposed on the Subprocessor; and

(b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4. **Opportunity to Object to Subprocessor Changes**.

(a) When any new Third Party Subprocessor is engaged during the Term, Processor will, at least 30 days before the new Third Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address.

(b) Customer may object to any new Third Party Subprocessor by terminating the Agreement immediately upon written notice to Processor, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 11.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12. **Processing Records**.

12.1. **Processor's Processing Records**. Customer acknowledges that Processor is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of processor and/or controller on behalf of which Processor is acting and, where applicable, of such processor's or controller's local representative and data protection officer, as well as the categories of processing carried out on behalf of each controller, where possible a general description of the technical and organisational security measures; and (b) make such information available to the supervisory authorities.

13. **Liability**.

13.1. **Liability Cap**. The total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the Agreement, the Data Processing Agreement, and the Model Contract Clauses (if such Model Contract Clauses have been entered into as described in Section 10.2 Transfers of Data

Out of the EEA) combined will be limited to the Agreed Liability Cap for the relevant party, subject to Section 13.2 (Liability Cap Exclusions).

13.2. **Liability Cap Exclusions**. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

14. **Effect of Agreement**. To the extent of any conflict or inconsistency between the terms of this Data Processing Agreement and the remainder of the Agreement, the terms of this Data Processing Agreement will govern.

15. Miscellaneous.

15.1. Neither the rights nor the obligations of any Party may be assigned in whole or in part without the prior written consent of the other Party, provided, however, that this Data Processing Agreement may be transferred or assigned in the event of a restructuring or change of control affecting a Party hereto.

15.2. In the event of any dispute arising between the Parties in connection with this Data Processing Agreement, the Parties shall negotiate in good faith to resolve their dispute. If the dispute cannot be resolved by good faith negotiations by the Parties, the dispute shall be finally settled by a public court relevant for the seat of the Processor.

15.3. This Data Processing Agreement is governed by laws of the state of Washington, without reference to its choice of law rules.

15.4. Should any provision of this Data Processing Agreement be invalid or unenforceable, then the remainder of this Data Processing Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

15.5. Any amendments to this Data Processing Agreement shall be made in writing, otherwise being null and void.

If you have any questions or concerns in regards to this Agreement, please contact privacy@defiant.com.

IN WITNESS WHEREOF, the Parties through their duly authorized representatives hereby agree to the terms of this Data Processing Agreement:

Defiant, Inc.

Sign: DocuSigned by: Kerry Boyte BA4076F1D16F4F5...

Name: Kerry Boyte

Title: COO, Defiant, Inc.

Customer: Petra

Sign: Pütz

Name: Digital unterschrieben von Petra Pütz
DN: cn=Petra Pütz, o=archaicARTs, ou, email=p.p@archaicarts.de, c=DE
Datum: 2018.06.17 20:23:02 +02'00'

Title:

Contact Email:

Date:

Appendix 1: Subject Matter and Details of the Data Processing (Record of Processing)

Subject Matter

Processor's provision of the Services and related technical support to Customer.

Duration of the Processing

The applicable Term plus the period from expiry of such Term until deletion of all Customer Data by Processor in accordance with the Data Processing Agreement.

Nature and Purpose of the Processing

Processor will process Customer Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to Customer in accordance with the Data Processing Agreement.

Categories of Data

When a Customer subscribes to or makes purchases through the Services, Defiant may collect name, email address, address, telephone number and payment information.

When a Customer uses specific features of the Services, Defiant may collect the following types of EU Personal Data:

When using the Services Defiant may collect the following Customer Data: originating Internet Protocol (IP) address, proxy IP address, url accessed, complete http header, http request body, and cookies (e.g., Google Analytics, Root Commerce (shopping cart contents), WordPress authentication cookie).

When using the site cleaning service, Defiant may download a complete copy of the Customer's website including the website database which may include Customer Data.

Defiant automatically collects Customer and End User search queries and the date and time of the Customer and/or End User's request and referral URL. Depending on the settings of a Customer and/or End User's computer or mobile device ("Device"), Defiant also automatically collects: IP address; MAC address; Device make, model and operating system version; mobile network information; internet service provider; browser type and language; country and time zone in which the Device is located; and metadata stored on the Device. When permitted, Defiant also may collect data about a User's geographic location through GPS, beacons and similar technology.

All of EU Personal Data is collected to operate, manage and improve the Services and ensure the technical functionality and security of the Services.

Data Subjects

EU Personal Data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As from the Agreement Effective Date, Processor will implement and maintain the Security Measures set out in this Appendix 2 to the Data Processing Agreement. Processor may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. Infrastructure security

Processor personnel are required to follow security policies that define access privileges and control for the transmission, processing, and storing of sensitive data. Processor conducts annual risk assessments on system and networking components which include systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media, where confidential, sensitive data is present.

Personnel are required to execute an Information Security policy and must acknowledge receipt of, and compliance with, Processor's security policies.

2. Personnel Security.

Processor personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Processor conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Processor's confidentiality and privacy policies.

3. Subprocessor Security.

Before onboarding Subprocessors, Processor conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Processor has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 11.3 (Requirements for Subprocessor Engagement) of this Data Processing Agreement, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Appendix 3: Subprocessors

Defiant uses the following subprocessors in the performance of the Service:

Subprocessor	Location
Amazon Web Services	United States
ByteGrid	United States
Twilio	United States
Freshworks	United States
Mode Analytics	United States

Standard Contractual Clauses (processors)

for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The Customer accepting the Clauses (the "Data Exporter")

And

Defiant, Inc.,
800 5th Ave Ste 4100, Seattle, WA 98104, USA
(the "Data Importer")

each a "party"; together "the parties",

AGREE on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1.

The Clauses (including appendices 1 and 2) are effective from the date the Customer entity has both: (i); executed a valid Wordfence terms of use agreement and data processing agreement (collectively the "Agreement") or is otherwise an authorized customer affiliate under such Agreement; and (ii) executed these Clauses agreement.

If you are executing on behalf of the Data Exporter, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms and conditions; (ii) you have read and understand the Clauses; and (iii) you agree, on behalf of the party that you represent, to the Clauses. The Clauses shall automatically expire on the termination or expiry of the Agreement.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '***personal data***', '***special categories of data***', '***process/processing***', '***controller***', '***processor***', '***Data Subject***' and '***Supervisory Authority***' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the ***Data Exporter***' means the controller who transfers the personal data;

(c) 'the ***Data Importer***' means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC;

(d) 'the ***Subprocessor***' means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the ***applicable data protection law***' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;

(f) '***technical and organisational security measures***' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The Data Subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.

3. The Data Subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the Data Importer or any Subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the Data Subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the personal data and the rights of Data Subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the Data Exporter about:

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

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal Data Subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the Data Exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;

(h) that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the processing services by the Subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any Subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Subprocessor is entitled to receive compensation from the Data Exporter for the damage suffered.

2. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.

3. If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the Subprocessor agrees that the Data Subject may issue a claim against the data Subprocessor with regard to its own processing operations under the Clauses as if it were the

Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. Without prejudice to paragraphs 1, 2 and 3 of Clause 6, each party's aggregate liability to the other under or in connection with these Clauses (whether in contract, tort or otherwise) is limited to the amount paid for the services by the Customer entity which is party to the Agreement in the 12 months immediately preceding the event (or first in a series of connected events) giving rise to the liability.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the Data Subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the Data Subject;

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

2. The parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of the Subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing Law

- The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-Processing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.

2. The prior written contract between the Data Importer and the Subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.

4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

IN WITNESS WHEREOF, the parties through their duly authorized representatives hereby agree to the terms of these Clauses:

DEFIANT, INC.	**DATA EXPORTER**
Sign: DocuSigned by: Kerry Boyte BA4076F1D16F4F5...	Sign: Petra Pütz Digital unterschrieben von Petra Pütz DN: cn=Petra Pütz, o=archaicARTs, ou, email=p.p@archaicarts.de, c=DE Datum: 2018.06.17 20:19:00 +02'00'
Name: Kerry Boyte	Name:
Title: COO, Defiant, Inc.	Title:

Appendix 1

to the Standard Contractual Clauses
This Appendix forms part of the Clauses

Data Exporter

- The Data Exporter is the Customer that is a party to the Clauses.

Data Importer

- The Data Importer is Defiant, Inc., a global provider of a variety of technology services for businesses.

Data Subjects

- The personal data transferred concern the Data Exporter's end users including employees and the Data Exporter's customers. Data Subjects also includes individuals collaborating and communicating with the Data Exporter's end users.

Categories of data

- When a Customer subscribes to or makes purchases through the Services, Defiant may collect name, email address, address, telephone number, and payment information.
- When a Customer uses specific features of the Services, Defiant may collect the following types of EU Personal Data:
- When using the Services Defiant may collect the following Customer Data: originating Internet Protocol (IP) address, proxy IP address, url accessed, complete http header, http request body, and cookies (e.g., Google Analytics, Root Commerce (shopping cart contents), WordPress authentication cookie).
- When using the site cleaning service, Defiant may download a complete copy of the Customer's website including the website database which may include Customer Data.
- Defiant automatically collects Customer and end user search queries and the date and time of the Customer and/or end user's request and referral URL. Depending on the settings of a Customer and/or end user's computer or mobile device ("Device"), Defiant also automatically collects: IP address; MAC address; Device make, model and operating system version; mobile network information; internet service provider; browser type and language; country and time zone in which the Device is located; and metadata stored on the Device. When permitted, Defiant also may collect data about a User's geographic location through GPS, beacons and similar technology.
- All of EU personal data is collected to operate, manage and improve the Services and ensure the technical functionality and security of the Services.

Special categories of data (if appropriate)

- The personal data transferred concern the special categories of data transmitted or displayed by end users via the Service.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

- Scope of Processing.
    - The Clauses reflect the parties' agreement with respect to the processing and transfer of personal data specified in this Appendix pursuant to the provision of the "Service" as defined under the Agreement.
    - Personal data may be processed for the following purposes: (a) to provide the Service, (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the Agreement.
    - The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its Subprocessors maintain facilities as necessary for it to provide the Service.
- Term of Data Processing.
    - Data processing will be for the term specified in the Agreement. For the term of the Agreement, and for a reasonable period of time after the expiry or termination of the Agreement, the Data Importer will provide the Data Exporter with access to, and the ability to export, the Data Exporter's personal data processed pursuant to the Agreement.
- Data Deletion.
    - For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to delete the Data Exporter's personal data from the Service. After termination or expiry of the Agreement, the Data Importer will delete the Data Exporter's personal data in accordance with the Agreement.
- Access to Data.
    - For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to correct, block, export and delete the Data Exporter's personal data from the Service in accordance with the Agreement.
- Subprocessors.
    - The Data Importer may engage Subprocessors to provide parts of the Service. The Data Importer will ensure Subprocessors only access and use the Data Exporter's personal data to provide the Service and not for any other purpose.

Appendix 2

to the Standard Contractual Clauses
This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

The Data Importer currently abides by the security standards as specified in the Agreement. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a material degradation in the security of the Service during the term of the Agreement.

Defiant Model Contract Clauses, Version 1.1