Data Processing Addendum

In providing the services described in our Terms of Service [https://en.wordpress.com/tos/][1] ("**Terms of Service**" or "**Agreement**"), we (the folks at Automattic) process personal data on behalf of the users of those services ("**Users**"), for which we act as the processor under applicable data protection laws and our users act as the controllers. That personal data is referred to as "**Controller Data**," as further described below.

This Data Processing Addendum ("**Addendum**") to our Terms of Service explains our data protection obligations and rights as a processor of the Controller Data, as well as the data protection obligations and rights of our Users as the controllers. Except in respect of the data protection obligations and rights of the parties set out in this Addendum, the provisions of the Agreement shall remain unchanged and shall continue in force.

For Users who reside in the United States or Brazil, this Addendum is between the User and Automattic Inc. (US), and for all other Users, this Addendum is between the User and Aut O'Mattic Ltd. (Ireland) (each, "**Automattic**" or "**we**").

1. Role of the Parties

Automattic and the User agree that with regard to the processing of the Controller Data, Automattic is the processor and the User is the controller.

2. Scope of the Processing

2.1. Automattic shall process the Controller Data on behalf of and in accordance with the instructions of the User. If Automattic is legally required to process Controller Data for another purpose, Automattic will inform the User of that legal requirement unless the law prohibits Automattic from doing so.

2.2. The processing of Controller Data by Automattic occurs for the purpose of providing Automattic's website creation and management services to our Users, and Controller Data is comprised exclusively of personal data relating to data subjects who use a User's website, which may include a User's customers, subscribers, followers, employees or other administrative users. Controller Data does not include content or personal data provided by any of the foregoing persons to Automattic in that person's capacity as a user of WordPress.com or another service provided directly to the person by Automattic.

[1] If you use our Polldaddy service, the Polldaddy Terms and Conditions at https://polldaddy.com/terms/ also apply. If you use Akismet, the Akismet Terms of Use at https://akismet.com/tos/ also apply. And if you use WooCommerce, the WooCommerce Use Terms at https://woocommerce.com/terms-conditions also apply.

The type of Controller Data processed by Automattic depends on the services and features that the User decides to implement for the User's website, and may include username and credentials; name; contact information, such as e-mail address, physical address, and telephone number; billing information, such as credit card data and billing address; website usage information, IP address, and other technical data such as browser type, unique device identifiers, language preference, referring site, the date and time of access, operating system, and mobile network information; approximate location data (from IP address); information regarding interactions with the website, such as "comments," poll responses, "ratings," and "likes"; and other information directly provided to the User's website by a visitor to the website, such as contact form submissions.

The duration of processing corresponds to the duration of the Agreement, which is described in the Terms of Service.

2.3. The instructions of the User are in principle conclusively stipulated and documented in the provisions of this Addendum. Individual instructions which deviate from the stipulations of this Addendum or which impose additional requirements shall require Automattic's consent.

2.4. The User is responsible for the lawfulness of the processing of the Controller Data. In case third parties assert a claim against Automattic based on the unlawfulness of processing Controller Data, the User shall release Automattic of any and all such claims.

2.5. Automattic reserves the right to anonymize the Controller Data or to aggregate data in a way which does not permit the identification of a natural person, as well as the right to use the data in this form for purposes of designing, further developing, optimizing, and providing its services to the User as well as to other users of the service. The parties agree that the Controller Data rendered anonymous or aggregated as above-mentioned are no longer classified as Controller Data in terms of this Addendum.

2.6. Automattic has the right to collect, use, and disclose any WordPress.com User Data in accordance with the Automattic privacy policy, which is available at https://automattic.com/privacy/. "**WordPress.com User Data**" means any information collected by Automattic from or about a visitor to User's website (including any contributor or editor), while that visitor is logged into a WordPress.com account. The Parties agree that Automattic's processing of WordPress.com User Data is independent of the services that Automattic provides to User for the User's website, and is not subject to this Addendum.

2.7. The parties further agree that Automattic's processing of data to deliver interest-based ads to the User's website, when such ads are enabled for free WordPress.com websites or on a website through WordAds or Jetpack Ads, is not subject to this Addendum.

3. Automattic's Personnel Requirements

3.1. Automattic shall require all personnel engaged in the processing of Controller Data to treat Controller Data as confidential.

3.2. Automattic shall ensure that natural persons acting under Automattic's authority who have access to Controller Data shall process such data only on Automattic's instructions.

4. Security of Processing

4.1. Automattic takes all appropriate technical and organisational measures, taking into account the state of the art, the implementation costs, and the nature, the scope, circumstances, and purposes of the processing of Controller Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subject, in order to ensure a level of protection appropriate to the risk of Controller Data.

4.2. In particular, Automattic shall establish prior to the beginning of the processing of Controller Data and maintain throughout the term the technical and organisational measures as specified in **Annex 1** to this Addendum and ensure that the processing of Controller Data is carried out in accordance with those measures.

4.3. Automattic shall have the right to modify technical and organisational measures during the term of the Agreement, as long as they continue to comply with the statutory requirements.

5. Further processors

5.1. The User hereby authorizes Automattic to engage further processors in a general manner in order to provide its services to the User. For Users whose Agreement is with Aut O'Mattic Ltd. (Ireland), the further processors currently engaged by Aut O'Mattic Ltd. (Ireland) include its related companies Automattic Inc. (US) and Bubblestorm Management Proprietary Limited (WooCommerce). The User may request a complete list of further processors from Automattic. In general, no authorization is required for contractual relationships with service providers that are not actively processing Controller Data but are only concerned with the examination or maintenance of data processing procedures or systems by third parties or that involve other additional services, even if access to Controller Data cannot be excluded, as long as Automattic takes reasonable steps to protect the confidentiality of the Controller Data.

5.2. Automattic shall inform the User of any intended changes concerning the addition or replacement of further processors. The User is entitled to object to any intended change. An objection may only be raised by the User for important reasons which have to be proven to Automattic. If the User objects, Automattic is prohibited from making the intended change. Insofar as the User does not object within 14 days after receipt of the notification, the User's right to object to the corresponding engagement lapses. If the User objects, Automattic is entitled to terminate the Agreement on reasonable notice.

5.3. The agreement between Automattic and further processors must impose the same obligations on the latter as those incumbent upon Automattic under this Addendum. The parties agree that this requirement is fulfilled if the contract has a level of protection corresponding to this Addendum and if the obligations laid down in applicable data protection laws are imposed on the further processor. In case Automattic engages a further processor outside of the EU, the User hereby authorises Automattic to conclude an agreement with another processor on behalf of the User based on the standard contractual clauses for the transfer of personal data to processors in third countries pursuant to the decision of the European Commission of February 5, 2010 ("**SCC**") and to specify the content of the SCC in accordance with this Addendum. The User hereby authorizes and instructs Automattic to exercise the User's rights under any SCC towards the further processors on its behalf in accordance with the instructions in this Addendum. Notwithstanding, Automattic may safeguard an adequate level of protection in a third country also by other means including binding corporate rules and other appropriate safeguards.

5.4. Automattic shall monitor the technical and organisational measures taken by the further processors.

6. Support obligations of Automattic

6.1. Automattic shall to a reasonable extent support the User with technical and organisational measures in fulfilling the User's obligation to respond to requests for exercising data subjects' rights.

6.2. Automattic shall notify the User promptly after becoming aware of any breach of the security of Controller Data in terms of Art. 4 no. 12 GDPR, in particular any incidents that lead to the destruction, loss, alteration, or unauthorized disclosure of or access to Controller Data. If possible, the notification shall contain a description of:

– the nature of the breach of Controller Data, indicating, as far as possible, the categories and the approximate number of affected data subjects, the categories and the approximate number of affected personal data sets;

– the likely consequences of the breach of Controller Data;

– the measures taken or proposed by Automattic to remedy the breach of Controller Data and, where appropriate, measures to mitigate their potential adverse effects.

6.3. In the event that the User is obligated to inform the supervisory authorities and/or data subjects in accordance with Art. 33, 34 of GDPR, Automattic shall, at the request of the User, assist the User to comply with these obligations.

7. Deletion and return of Controller Data

Upon termination of the Terms of Service Automattic shall delete all Controller Data, unless Automattic is obligated by law to further store Controller Data.

8. Evidence and audits

8.1. Automattic shall ensure that the processing of Controller Data is consistent with this Addendum.

8.2. Automattic shall document the implementations of the obligations under this Addendum in an appropriate manner and provide the User with appropriate evidence at the latter's reasonable request.

8.3. At the User's reasonable request, Automattic shall demonstrate compliance with the obligations under this Addendum by submitting an opinion or report from an independent authority (e.g. an auditor) or a suitable certification by IT security or data protection audit relating to an inspection carried out in relation to Automattic's data processing systems ("audit report").

[Signatures on the following page]

USER User Legal Name: _____ _____ Signatory Name: _____ Title: _____ Date: _____	**AUTOMATTIC INC.** _____ Signatory Name: _____ Title: _____ Date: _____
	AUT O'MATTIC LTD. (IRELAND) _____ Signatory Name: _____ Title: _____ Date: _____

Annex 1

Automattic maintains commercially reasonable safeguards designed to protect Controller Data from unauthorised access, use and disclosure. Automattic currently abides by the security standards below. Automattic may update or modify these security standards from time to time, provided that such updates and modifications will not result in a degradation of the overall security of Automattic's services during the term of the User's Agreement with Automattic.

1. Information Security Organisational Measures

- Automattic has a dedicated security team committed to protecting Controller Data which works with our product teams to address potential security risks.
- Automattic performs regular internal security testing and engages with third parties to perform application and network vulnerability assessments.
- Automattic requires all employees with access to Controller Data to observe the confidentiality of that data, and trains employees on confidentiality and security.
- Automattic uses commercially reasonable measures for software, services, and application development, including routine dynamic testing and training personnel on coding techniques that promote security.

2. Physical Security

- Automattic's servers are co-located in data centers designed to meet the regulatory demands of multiple industries. All servers are housed in dedicated cages to separate our equipment from other tenants.
- Automattic's origin servers currently meet the International Organization of Standardization (ISO), International Electrotechnical Commission (IEC) 27001 certification, Standards for Attestation Engagements (SSAE) No. 16 (SOC1) and SOC2 Type 2, and ongoing surveillance reviews.
- Automattic limits access to facilities where information systems that process Controller Data are located to identified, authorized individuals via measures which may include identity cards, security locks, key restrictions, logging of access, security alarm systems, and surveillance cameras.

3. Access Controls

- Automattic runs network firewalls and host based firewalls (if applicable) and has real time processes designed to provide alerts for unauthorized access attempts. Automattic also has commercially reasonable security measures in place to help protect against denial of service (DDos) attacks.
- Automattic maintains commercially reasonable access control procedures designed to limit access to Controller Data, including processes addressing password and account

management for employees with access to Controller Data, virus scanning, and logging access to Controller Data.

- Automattic encrypts (serve over SSL) all WordPress.com websites, including custom domains hosted on WordPress.com.

4. Data Backup and Recovery

- Automattic uses industry standard systems to help protect against loss of Contoller Data due to power supply failure or line interference, which may include fire protection and warning measures, emergency power generators, and data recovery procedures.