Automattic Data Processing Addendum

This Data Processing Addendum ("**Addendum**" or "**DPA**") is entered into by and and Automattic Inc. or Aut O'Mattic A8C Ireland Ltd. (as applicable, "Automattic") and the Company using the WP Cloud Services, on behalf of itself and its affiliates (collectively, "**Company**"). Automattic and Company are parties to an agreement (the **"Agreement"**) pursuant to which Automattic provides certain services (the **"Services"**) to Company. Automattic processes Personal Data on behalf of Company when providing such Services and acts as the processor under applicable Data Protection Laws. Company acts as controller. That personal data is referred to as "**Company Data**," as further described below.

This Addendum explains Automattic's data protection obligations and rights as a processor of the Company Data, as well as the data protection obligations and rights of Company as the controller. 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.

"Data Protection Laws" means any and all privacy, security and data protection laws and regulations that apply to the Personal Data processed by the processor under the Agreement, including, as applicable: (1) the GDPR means the General Data Protection 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 date, (2) Member State laws implementing the GDPR, and (3) the CCPA which means the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq, including any subsequent amendments or addendums.

"Personal Data" means any information relating to an identified or identifiable natural person or that is otherwise deemed personal information or personal data (or similar variations of those terms) under Data Protection Laws.

"Controller-to-Processor Clauses" in relation to the Processing of Personal Data pursuant to this DPA means the model clauses, as applicable, set forth in Attachment 1.

Role of the Parties. In this Agreement, the term "Parties" refers collectively to Automattic and the Company. The Parties agree that with regard to the processing of the Controller Data, Automattic is the processor and Company is the Controller.

1. Scope of the Processing

1.1. Company may provide Automattic with Personal Data about Company's own users as well as users of Company's websites as collected by Company on its websites ("Company Data"). Automattic shall process the Company Data on behalf of and in accordance with Company's instructions. If Automattic is legally required to process Company Data for another purpose, Automattic will inform Company of that legal requirement unless the law prohibits Automattic from doing so.

1.2. Automattic will not: (a) collect, retain, use, disclose or otherwise process the Company Data for any purpose other than as necessary for the specific purpose of performing the Services on behalf of the Company; (b) collect, retain, use or disclose the Company Data for a commercial purpose other than providing the Services on behalf of Company; or (c) "sell" the Company Data as defined in the CCPA.

1.3. The processing of Company Data by Automattic occurs for the purpose of providing Automattic's website hosting and support services, and Company Data is comprised exclusively of personal data relating to data subjects who use a Company website, which may include Company's Companys and end users. Company 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.

Company may collect Company Data when, for example, (1) an end user creates an account with the Company (for clarity, not a WordPress.com account); (2) a Company administrator adds content to the site that may include Company Data, or (3) Company provides directory or other information about its end users as part of an intranet (i.e., a website that is only accessible to authorized, internal personnel) used by Company. The type of personal data collected depends on the services and features that the Company decides to implement for the Company's website, but typically includes personal data that allows the Company's Companys and end users to access and use the Company's websites, such as username and e-mail address.

The duration of processing corresponds to the duration of the Agreement. Termination of the Agreement is described in the Agreement.

1.4. The instructions of the Company 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 agreement. Automattic will immediately inform the Company if, in Automattic's opinion, an instruction from the Company infringes applicable data protection law.

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

1.6. Company agrees that Automattic may depersonalise the Company Data or aggregate data in a way which does not permit the identification of a natural person, as well as to use the data in this form for purposes of designing, further developing, optimizing, and providing its services to the Company as well as to other users of the service. The parties agree that the Company Data rendered depersonalised or aggregated as above-mentioned are no longer classified as Company Data in terms of this Addendum and that Automattic is instructed by Company to depersonalise Company Data in accordance with this clause.

1.7. Automattic has the right to collect, use, and disclose any WordPress.com Company data ("Company Data") which is distinct from Company Data in accordance with the Automattic privacy policy, which is available at https://automattic.com/privacy/. Company Data includes any information collected by Automattic from or about a visitor to Company'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 Company Data is independent of the services that Automattic provides directly to the Company for the Company's website, and is not subject to this Addendum.

2. Automattic's Personnel Requirements

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

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

3. Security of Processing

3.1. Automattic takes 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 Company 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 Company Data.

3.2. Automattic shall secure Company Data in accordance with all requirements under the Data Protection Laws. In particular, Automattic shall establish prior to the beginning of the processing of Company Data, and maintain throughout the term of such processing, the technical and organisational measures as specified in **Appendix 1** to this Addendum and ensure that the processing of Company Data is carried out in accordance with those measures.

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

4. Further processors

4.1. The Company hereby authorizes Automattic to engage further processors, including Automattic Inc., in a general manner in order to provide its services to the Company. The Company may view a complete list of further processors engaged by Automattic (**https://Automattic.com/subprocessors/)**. In general, no authorization is required for contractual relationships with service providers that are not actively processing Company 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 Company Data cannot be excluded, as long as Automattic takes reasonable steps to protect the confidentiality of the Company Data.

4.2. Automattic shall inform the Company of any intended changes concerning the addition or replacement of further processors. The Company is entitled to object to any such intended change but only to the extent that it has a reasonable basis for doing so. Insofar as the Company does not object within 14 days of Automattic's notification of such change, the Company's right to object to the corresponding engagement lapses. If the Company objects to a change in a timely fashion, and if the Parties are unable to resolve such objection in a timely manner, Automattic shall be entitled to terminate the Agreement upon reasonable notice in which case Automattic shall have no liability with respect to such termination.

4.3. The agreements 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 European Economic Area, the Company hereby instructs and authorises Automattic to conclude an agreement with another processor on behalf of the Company based on the Standard Contractual Clauses for the transfer of personal data to processors in third countries. As the case may be, where the Company Data requires additional protection under the Standard Contractual Clauses in order to provide for appropriate safeguards according to applicable data protection laws, Automattic shall ensure any further processor it engages is bound by the Standard Contractual Clauses (processor to processor Standard Contractual Clauses). Notwithstanding the foregoing, Automattic may also ensure an adequate level of protection in a country outside of the European Economic Area by other means including binding corporate rules and other appropriate safeguards.

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

5. Support obligations of Automattic

5.1. Automattic shall provide assistance to the Company pursuant to its obligations under Article 28 GDPR.

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

5.3. Automattic shall notify the Company promptly after becoming aware of any breach of the security of Company Data, in particular any incidents that lead to the destruction, loss, alteration, or unauthorized disclosure of or access to or use of Company Data (each, a "Security Incident"). The notification shall contain a description of:

5.3.1. the nature of the breach of Company 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;

5.3.2. the likely consequences of the breach of Company Data; and

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

5.4. The above details may be provided in multiple notifications as the information becomes available. In the event that the Company is obligated to inform the supervisory authorities and/or data subjects of a Security Incident, Automattic shall, at the request of the Company, assist the Company to comply with these obligations.

5.5. Automattic will take appropriate steps to promptly remediate the cause of any Security Incident and will reasonably cooperate with the Company with respect to the investigation and remediation of such incident, including providing such assistance as required to enable the Company to notify and cure an alleged violation of Data Protection Law related to a Security Incident. Automattic will not engage in any action or inaction that unreasonably prevents the Company from curing an alleged violation of Data Protection Law.

6. Termination; Deletion and return of Company Data

This Addendum shall remain in effect for as long as Automattic carries out processing of Company Data or until termination of the Agreement and, in any event, until all Company Data has been deleted in accordance with this Section 6. Upon termination of the Agreement, Automattic shall delete all Company Data, unless Automattic is obligated by law to further store Company Data.

7. Evidence and audits

7.1. Automattic shall ensure that the processing of Company Data is consistent with this Addendum.

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

7.3. At the Company'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 auditors, relating to an inspection carried out in relation to Automattic's data processing systems.

8. Standard Contractual Clauses Transfers

8.1. As the case may be, the Company Data requires additional protection under the Standard Contractual Clauses in order to provide for appropriate safeguards according to applicable Data Protection Laws. Against this background, Automattic agrees to be bound by the Standard Contractual Clauses as per **Appendix 2** and agrees to comply with all obligations that are imposed on the data importer under the Standard Contractual Clauses with respect to Company Data.

Appendix 1

Security is a shared responsibility between Automattic and the Company. Automattic's WP Cloud Hosting Service is designed to provide a secure platform where Company may build and manage secure and scalable WordPress applications. Automattic manages and monitors the environment where our Company websites run, including the physical servers, operating system, and network layers of the WP Cloud Hosting Service.

Additionally, Automattic provides tools, support, and resources designed to enable Company to maintain the security of their WordPress websites.

Automattic makes security a priority and is committed to offering Company a platform that aims to protect the security of the Company's site and data. This document describes some of the measures Automattic has implemented, and some that Automattic recommends Company implement to help keep their sites and applications secure. **No matter what Automattic does, no method of transmission over the Internet and no method of electronic storage is perfectly secure. Automattic cannot guarantee absolute security of the Company's site or account - no one can.**

Company Responsibilities

Company should help to keep its account secure by using sufficiently complicated passwords, not reusing passwords across services, enabling two-factor authentication, and storing passwords safely. Company should also ensure that it employs sufficient security measures on its own systems.

SSL

Automattic strongly recommends enabling SSL (HTTPS) on all Company websites hosted by Automattic. At a minimum, Automattic uses SSL and HTTPS for all authenticated Company access to our services.

Automattic can obtain and implement auto-renewing SSL certificates from Let's Encrypt (https://letsencrypt.org/) as part of our service. The Company may also purchase their own certificate from any SSL vendor.

Network Security

- **Firewalls:** Automattic runs network and host based firewalls and has real time processes designed to provide alerts for unauthorized access attempts.
- **DDoS Protection:** All WP Cloud Hosting sites include measures designed to protect against distributed denial of service (DDoS) attacks.
- **CDN:** WP Cloud Hosting includes use of Automattic's globally distributed content delivery network (CDN) which is designed to enable Automattic's Cloud Hosting sites to operate at the fastest possible speeds, regardless of location.
- **Logging and Auditing:** Automattic logs activity at the application (WordPress), web server (nginx), load balancing (nginx), database (MySQL), and operating system layers (Linux). This allows Automattic to analyze and investigate security issues. Each layer of the stack logs to the local environment in real time. Logs are backed up daily and retained for 30 days.

Data Security

- **Application:** In order to help maintain secure, performant environments for the Company, each WordPress instance on the WP Cloud Hosting Service runs within its own isolated, containerized environment and cannot interact with other applications or areas of the system. These containers isolate processes, memory, as well as the file system.
- **Database:** Databases are set up per application to help mitigate the risk of unauthorized access between applications and each database requires its own unique authentication.

- **Company Data Access:** Normal operations of the WP Cloud Hosting Service include application support in the form of troubleshooting, platform upgrades, testing, and code review. Company data is access controlled and is designed to be limited to those Automattic employees performing such activities.

Vulnerability Management

- **Patching:** Automattic actively monitors for security patch releases and applies identified patches where appropriate to its operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities. Automattic prioritizes patching based on severity and impact on the Company's security.
- **Security Testing:** Automattic performs regular internal security testing and engages with third parties to perform application and network vulnerability assessments.
- **Penetration Testing:** Automattic is happy to work with the Company who is interested in performing their own independent penetration testing.
- **Bug Bounty:** Automattic takes the security of its platforms very seriously. Automattic operates a bug bounty program via HackerOne to reward those who find bugs and help improve the security of our applications.
- **Viruses/Malware:** Automattic makes available anti-malware controls, as well as antivirus tests that the Company can enable to help secure code deployed to our platform.
- **Personnel**: Automattic's security team is led by its Security Czar and is responsible for Automattic's application and information security. This security team works directly with Automattic's product teams and Companys to address risk and maintain Automattic's strong commitment to keeping its products safe.

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 Automattic's equipment from other tenants. Automattic's data centers currently meet the International Organization of Standardization (ISO), International Electrotechnical Commission (IEC) 27001 certification, Standards for Attestation Engagements (SSAE) No. 18 (SOC1) and SOC2 Type 2, and ongoing surveillance reviews.
- Automattic limits access to facilities where information systems that process Company Data are located to identified authorized individuals.
- Automattic uses a variety of industry standard systems to help protect against loss of data due to power supply failure or line interference.

Data Deletion, Backup, and Recovery

- Automattic backup systems are designed to backup Company site data on an hourly basis.
- Automattic maintains emergency and contingency plans for the facilities in which data is located including redundant storage and procedures for recovering data that are designed to attempt to reconstruct data in its original or last-replicated state from before the time it was lost.
- The Company may choose to delete content published on Automattic's service; upon deletion Automattic will clear deleted content from its internal cache within 2 business days, but deleted content may not be cleared as quickly from external caches (for example, Google search index).
- The Company may also request deletion of any personal data (for example, the names and email addresses of Company's own users) that it provided to Automattic and/or stored on Automattic.

Certifications

All of Automattic's data centers have committed to maintain SSAE18 SOC 1, SSAE SOC 2 certifications.

How We Handle Service Disruptions

- In the event of a disruption to the WP Cloud Hosting Service, Automattic will, as soon as reasonably practical, provide information on the nature of the disruption, the steps being taken to remedy the disruption, and the expected duration of the disruption (if possible).
- Information and updates will be provided by email to the address we have on file for the Company account.

ATTACHMENT 1

STANDARD CONTRACTUAL CLAUSES

The Parties agree that the Processor to Controller Standard Clauses are incorporated into the DPA by reference, as if they had been set out in full with the following specifications.

(a) Specifications to Relevant Provisions in Module Two:

(i) *Clause 7 (Optional Docking clause).* Clause 7 is omitted.

(ii) *Clause 13 (Supervision).* Clause 13(a) shall read as follows: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(iii) *Clause 17 (Governing law).* Clause 17 shall read as follows: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

(iv) *Clause 18 Choice of forum and jurisdiction.* Clause 18(b) shall read as follows: The Parties agree that those shall be the courts of the Republic of Ireland.

(b) Annexes I and II follow in the Appendix on the next page.

APPENDIX

ANNEX I

A. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customers of controller; data subjects discussed in the contents of Company's websites; Company's end users (e.g. customers, subscribers, followers, employees or other administrative users).

Categories of personal data transferred

The type of personal data collected depends on the services and features that the Company decides to implement for the Company's website, but typically includes personal data that allows the Company's customers and end users to access and use the Company's websites, such as username and credentials; name; contact information, such as e-mail address and password hashes. The personal data may also be included in content (text and media) on Company's sites.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuously.

Nature of the processing

Collection, use, organisation, and storage.

Purpose(s) of the data transfer and further processing

The data processing provided for by these standard contractual clauses is executed for the purpose of providing the services described in the WP Cloud Services Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Subject to any legal requirement to keep personal data, we discard personal data when no longer needed for the purposes described in the WP Cloud Services Agreement. Upon termination of the Agreement, Automattic shall delete all Company's personal data, unless Automattic is obligated by law to further store Company's personal data.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Amazon Web Services - the above categories and data subjects, and for encrypted offsite back-ups only and for as long as the services agreement is in effect between controller and processor.

Automattic Inc. - the above categories, data subjects and duration, and for use of data centers.

List of Subprocessors can be seen here: https://Automattic.com/subprocessors/

B. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority of the Company's main establishment.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organisational measures taken by Automattic are as described in Appendix 1 above.