Data Processing Addendum

Version 1

Controller and **Processor** agree to add the following terms to their Services Agreement:

1. *Operational Details*.

(a) *Processing Summary*.

(i) *Controller Activities*. [Describe what the Controller does and how they will use the forum.]

(ii) *Processor Activities*. Processor will host an Internet discussion forum for Controller using its Discourse forum software.

(iii) *Categories of Data Subjects*. Processor will Process data relating to users of Controller's forum and Controller personnel administering and using the forum.

(iv) *Categories of Data*. Processor will Process data about visits to Controller's forum, account data for forum users, and data about posts and other activity on the forum.

(v) *Special Categories of Data*. Neither Controller nor Processor will solicit or intentionally collect special categories of data as part of activities within the scope of the Services Agreement.

(vi) *Processing Operations*. Processor's Discourse forum software will Process data collected in order to provide Controller's forum. The Discourse forum software will store the data, analyze it to prevent spam posts and determine forum user trust and privileges, and distribute it to content delivery networks worldwide for fast access.

(vii) *Duration of Processing*. Processor will Process data for the term of the Services Agreement.

(viii) *Obligations*. The Services Agreement and this addendum set out the obligations and rights of Processor and Controller.

(b) *Security Measures*. Processor has implemented and shall maintain a written security program that includes appropriate administrative, physical, and technical safeguards designed to protect Controller Personal Data from Personal Data Breaches and to help ensure the ongoing confidentiality, integrity, and availability of the Customer Data and Processing systems. These safeguards include:

(i) User authentication and authorization to ensure data is only accessed by those with a legitimate need to do so.

(ii) Use of encryption where appropriate to secure data in transit and at rest, including on staff mobile devices.

(iii) Security measures to limit access to the facilities and devices involved in storing data, such as physical access controls at data centers and network firewalls.

(iv) Training for all staff to ensure awareness of security best practices.

(v) A public bug bounty program for the Discourse forum software, to ensure security issues are identified and remediated quickly.

(c) *Assistance Responding to Data Subject Rights*.

(i) Processor will provide Controller an e-mail address to which Controller can address requests for assistance with Data Subject rights requests.

(ii) Processor's Discourse forum software will provide Controller forum administrators with the ability to change and delete some Personal Data without Processor's assistance.

2. *Processing of Controller Personal Data*.

(a) *Compliant Processing*. Processor and each Subprocessor agree to:

(i) comply with all applicable Data Protection Law in the Processing of Controller Personal Data; and

(ii) not Process Controller Personal Data other than on the relevant Controller Company's written instructions, unless Processing is required by law, in which case the Processor or Subprocessor agrees to give the Controller Company notice of the legal requirement before Processing, if the law permits.

(b) *Instruction to Process*. Each Controller Company instructs Processor, and authorizes Processor and each Subprocessor to instruct each of their Subprocessors, to Process Controller Personal Data and transfer Controller Personal Data to any country or territory as necessary for the provision of the Services, consistent with the Services Agreement.

(c) *Legal Instruction Warranty*. Each Controller Company states that it is and will be legally authorized to give the instruction in *Section 2(b) (Instruction to Process)*.

(d) *Required Information*. *Section 1(a) (Processing Summary)* sets out information required by GDPR 28(3). Controller can make amendments to *Section 1(a) (Processing Summary)* by written notice to Processor as necessary to meet similar requirements of other Data Protection Law. Nothing in *Section 1(a) (Processing Summary)* confers any right or imposes any obligation on any party to this addendum.

3. *Personnel*. Processor agrees to:

(a) answer for breaches of this addendum by its Personnel, and Personnel of any Subprocessor, with access to Controller Personal Data;

(b) limit access to Controller Personal Data to Personnel who need access for purposes of the Services Agreement, or to comply with Data Protection Law; and

(c) ensure that all Personnel with access to Controller Personal Data have obligations to keep them confidential under contracts, professional obligations, or legal requirements.

4. *Security*. Processor agrees to implement the security measures listed in *Section 1(b) (Security Measures)* for the protection of Controller Personal Data.

5. *Subprocessing*.

   (a) *Appointing Subprocessors*. Each Controller Company authorizes Processor to appoint Subprocessors, and each of the Subprocessors to appoint Subprocessors in turn, and so on, under *Section 5 (Subprocessing)* and any restrictions in the Services Agreement.

   (b) *Current Subprocessors*. Processor may continue to use Subprocessors they were using before signing this addendum, as long as those Subprocessors meet the requirements of *Section 5(d) (Subprocessor Requirements)*. Among those, Processor may continue to use:

      (i) Digital Ocean, for creating, storing, and managing data backups

      (ii) Automattic, Inc., for Akismet spam detection and Gravatar user avatars

      (iii) Amazon Web Services, for data backup and fast worldwide distribution of Discourse forum content to web visitors

      (iv) Hurricane Electric, for Internet access, server colocation in the United States, or both

      (v) Equinix, for server colocation in the European Union

      (vi) Google, Inc., for notifications to users of the Discourse app for Android devices via Google Cloud Messaging

      (vii) Apple, Inc., for notifications to users of the Discourse app for iOS devices via Apple Push Notification Service

      (viii) KeyCDN, for fast worldwide distribution of Discourse forum content to web visitors

   (c) *Notice and Objection*. Processor agrees to give Controller prior written notice of the appointment of any new Subprocessor, describing the Processing the Subprocessor will do. If Controller gives Processor notice of a reasonable objection within fourteen calendar days:

      (i) Processor agrees to work with Controller to change how it provides the Services, to avoid using the new Subprocessor.

      (ii) If Processor cannot make such a change within thirty calendar days, Controller may terminate the Services Agreement to the extent of the Services that require the new Subprocessor.

   (d) *Subprocessor Requirements*. Processor or any Subprocessor appointing any new Subprocessor must:

      (i) perform adequate due diligence to ensure the new Subprocessor can provide the level of protection for Controller Personal Data required by the Services Agreement and this addendum, before that new Subprocessor Processes any Controller Personal Data.

(ii) ensure the relationship with the new Subprocessor is governed by a written contract:

(A) requiring at least the same level of protection for Controller Personal Data as this addendum; and

(B) meeting the requirements of GDPR 28(3);

(iii) ensure the Standard Contractual Clauses are part of the contract with the new Subprocessor at all times while the new Subprocessor Processes Controller Personal Data, if the relationship involves any Restricted Transfer; and

(iv) give the Controller review copies of the contract with the new Subprocessor on request, optionally redacted to remove confidential information not relevant to compliance with this addendum.

(e) *Subprocessor Compliance*. Processor agrees to ensure that each Subprocessor will abide by the following sections, as if the Subprocessor were the Processor, to the extent they apply to Processing the Subprocessor does:

(i) *Section 2(a) (Compliant Processing)*;

(ii) *Section 3 (Personnel)*;

(iii) *Section 4 (Security)*;

(iv) *Section 6 (Data Subject Rights)*;

(v) *Section 7 (Data Breach)*;

(vi) *Section 8 (Impact Assessment and Prior Consultation)*;

(vii) *Section 9 (Deletion or Return)*; and

(vii) *Section 10(a) (Audit Obligations)*.

6. *Data Subject Rights*.

(a) Processor agrees to implement the appropriate technical and organizational measures listed in *Section 1(c) (Assistance Responding to Data Subject Rights)* to help each Controller Company meet its obligation to respond to requests to exercise Data Subject rights under Data Protection Law.

(b) Processor agrees to:

(i) notify Controller promptly if Processor or any Subprocessor receives a request from a Data Subject under Data Protection Law about Controller Personal Data; and

(ii) ensure that the recipient does not respond to that request unless required by Data Protection Law, except on written instructions from the Controller or the relevant Controller Affiliate.

(c) If Data Protection Law permits, Processor agrees to notify Controller before a Processor or any Subprocessor responds to a request because they are required to do so by Data Protection Law.

7. *Data Breach*.

(a) *Data Breach Notice*. Processor agrees to notify Controller without undue delay when Processor or any Subprocessor becomes aware of a Personal Data Breach affecting Controller Personal Data. As the information becomes available, Processor agrees to notify Controller of:

(i) the nature of the Personal Data Breach;

(ii) the estimated categories and number of Data Subjects affected;

(iii) the estimated categories and number of Personal Data records affected;

(iv) contact information for Personnel who can answer further questions; and

(v) measures taken or planned to address the Personal Data Breach.

(b) *Data Breach Cooperation*. Processor agrees to cooperate with each Controller Company to investigate, mitigate, and remediate any Personal Data Breach.

8. *Impact Assessment and Prior Consultation*. Processor agrees to assist each Controller Company with data protection impact assessments and prior consultations with any Supervisory Authority or other competent data privacy authority required by GDPR 35, GDPR 36, or similar provisions of other Data Protection Law, by answering questions about the Processing of Controller Personal Data by Processor and any Subprocessor.

9. *Deletion or Return*.

(a) *Obligation to Delete*. Subject to *Section 9(b) (Option to Return)* and *Section 9(c) (Data Retention)*, Processor agrees to delete all copies of Controller Personal Data, and to require every Subprocessor to delete all copies, within thirty calendar days of the End of Services.

(b) *Option to Return*. Subject to *Section 9(c) (Data Retention)*, Controller may give Processor notice within fourteen calendar days of the End of Services that Processor must instead return one complete copy of all Controller Personal Data to Controller by secure file transfer in standard file formats, delete other copies, and require every Subprocessor to delete other copies. Processor agrees to return the copy requested within thirty calendar days of the End of Services.

(c) *Data Retention*. Processor and each Subprocessor may retain Controller Personal Data as required by Data Protection Law. Processor and each Subprocessor retaining Controller Personal Data agree to keep them confidential, and to ensure they are only Processed as necessary for purposes required by Data Protection Law.

(d) *Certificate of Deletion or Return*. Processor agrees to certify to Controller in writing that Processor and all Subprocessors have fully complied with *Section 9 (Deletion or Return)* within sixty calendar days of the End of Services.

10. *Audit*.

(a) *Audit Obligations*. To the extent information and audit rights under the Services Agreement fall short of what GDPR 28(3)(h) and similar provisions of other Data Protection Law require, Processor agrees to:

(i) provide information on request from any Controller Company to demonstrate compliance with this addendum; and

(ii) grant access for, and cooperate with, audits and inspections of compliance with this addendum by any Controller Company or Controller Company auditor.

(b) *Audit Procedure*.

(i) *Notice of Audit*. Each Controller Company agrees to give Processor prior written notice of any audit or inspection under *Section 10(a) (Audit Obligations)*.

(ii) *Minimize Disruption*. Each Controller Company agrees to ensure that Controller Company Personnel and auditor Personnel take reasonable steps to avoid and minimize damage, injury, and disruption to the premises, equipment, personnel, and business of Processor and every Subprocessor.

(iii) *Audit Limits*. Neither Processor nor any Subprocessor has to give access for an audit or inspection:

(A) to anyone without reasonable evidence of identity or authority;

(B) outside normal business hours, unless the Controller Company performing the audit gave prior notice that the audit or inspection needs to be conducted on an emergency basis; or

(C) more than once per calendar year, not counting audits or inspections for which the Controller Company mentions in its notice that:

(I) the Controller Company considers the audit necessary because of concerns about compliance with this addendum;

(II) Data Protection Law requires the Controller Company to perform the audit; or

(III) a Supervisory Authority or similar regulatory authority responsible for enforcing Data Protection Law requests or requires the Controller Company to perform the audit.

11. *Restricted Transfers*.

(a) *Standard Contractual Clauses*. Subject to *Section 11(b) (Standard Contractual Clauses Apply Only if Necessary)*, each Controller Company (as data exporter) and Processor (as data importer) agree to the Standard Contractual Clauses for any Restricted Transfer from Controller Company to Processor, substituting *Section 1(a) (Processing Summary)* for appendix 1 and *Section 1(b) (Security Measures)* for appendix 2 to the Standard Contractual Clauses.

(b) *Standard Contractual Clauses Apply Only if Necessary*. *Section 11(a) (Standard Contractual Clauses)* applies to a Restricted Transfer only if necessary, together

with other practical compliance steps, short of getting Data Subjects' consent, to make the relevant Restricted Transfer legal under Data Protection Law.

12. *General Terms*.

(a) *Governing Law and Jurisdiction*. Other than under the "Mediation and Jurisdiction" and "Governing Law" clauses of the Standard Contractual Clauses, the dispute resolution, venue, and forum provisions of the Services Agreement apply to this addendum.

(b) *Order of Precedence*.

(i) *Standard Contractual Clauses Trump this Addendum*. Where this addendum and the Standard Contractual Clauses conflict, the Standard Contractual Clauses take precedence.

(ii) *No Effect on Services Agreement Scope*. Nothing in this addendum reduces any Processor data protection obligations under the Services Agreement or permits Processor to Process or allow Processing of Personal Data in any way the Services Agreement prohibits.

(iii) *This Addendum Trumps Other Agreements*. Subject to *Section 12(b)(ii) (No Effect on Services Agreement Scope)*, where this addendum conflicts with other agreements between the parties, such as the Services Agreement, signed before or after this addendum, this addendum takes precedence.

(c) *Changes in Data Protection Law*.

(i) *Amendments for Compliance*. Controller may amend the Standard Contractual Clauses as required by a change in Data Protection Law, or a court or regulator decision under Data Protection Law, to allow Restricted Transfer to continue without breaching Data Protection Law. Controller must give Processor notice thirty calendar days in advance.

(ii) *Amendments to Address New Risks*. If Controller gives notice under *Section 12(c)(i) (Amendments for Compliance)*, Controller agrees not to unreasonably withhold or delay agreement to any amendments to this addendum proposed by Processor to protect Processor or any Subprocessor from additional risks posed by the amendment to the Standard Contractual Clauses.

(iii) *Good Faith Negotiation*. If Controller gives notice under *Section 12(c)(ii) (Amendments to Address New Risks)*, the parties agree to negotiate amendments to address the requirements identified in Controller's notice in good faith, as soon as practical.

(iv) *Amendment without Affiliates*. Neither Controller nor Processor needs the consent or approval of any Affiliate to amend this addendum, including under *Section 12(c)(ii) (Amendments to Address New Risks)*.

(d) *Severance*. The parties intend that:

(i) any part of this addendum held invalid or unenforceable be changed to the minimum extent necessary to make it enforceable;

(ii) any part of this addendum that cannot be changed to make it enforceable be disregarded; and

(iii) the rest of this addendum remains in force, unless that frustrates the essential purpose of this addendum: to meet the requirements of Data Protection Law for Processing of Controller Personal Data as part of the Services.

13. *Definitions*.

(a) **Affiliate** means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with another entity, where control means having direct or indirect power to direct the management and policies, through ownership of voting securities, contract, or otherwise.

(b) **Services Agreement** means the agreement for services between Controller and Processor, signed before this addendum or along with it.

(c) **End of Services** means the date Processor stops providing Services under the Services Agreement.

(d) **Controller Affiliate** means an Affiliate of Controller.

(e) **Controller Company** means Controller or any Controller Affiliate.

(f) **Controller Personal Data** means any Personal Data related to the Services Agreement Processed by Processor or any Subprocessor on behalf of a Controller Company.

(g) **Data Protection Law** means data protection laws of the European Union, European Union Member States, Switzerland, and the United Kingdom, to the extent they apply to Processing of Controller Personal Data.

(h) **GDPR** means EU General Data Protection Regulation 2016/679.

(i) **Personnel** means employees, agents, and contractors.

(j) **Restricted Transfer** means either:

(i) a transfer of Controller Personal Data from any Controller Company to Processor or any Subprocessor; or

(ii) an onward transfer of Controller Personal Data

that Data Protection Law or transfer agreements under Data Protection Law would prohibit without Standard Contractual Clauses, whether from Processor to a Subprocessor, from Subprocessor to Subprocessor, or between establishments of Processor or a Subprocessor.

(k) **Services** means services provided under the Services Agreement.

(l) **Standard Contractual Clauses** means the standard contractual clauses for the transfer of personal data to processors established in third countries from Commission decision 2010/87/EU, in the English language.

(m) **Subprocessor** (plural **Subprocessors**) means anyone appointed by or on behalf of Processor to Process Controller Personal Data on behalf of any Controller Company in connection with the Services Agreement.

(n) **Commission**, **Data Subject** (plural **Data Subjects**), **Member States**, **Personal Data**, **Personal Data Breach**, **Processing**, and **Supervisory Authority** have the same meanings as in GDPR.

[Signature page follows.]

The parties are signing this data processing addendum on the dates by their signatures.

Processor:

WoW Lazy Macros

By:

Name:

Title:

Date:

Controller:

[Legal Name]

a [Jurisdiction] [Legal Form]

By:

Name:

Title:

Date: