

## Data Processing Addendum

In providing the services described in our Terms of Service <https://wordpress.com/tos/><sup>1</sup> (“**Terms of Service**” or “**Agreement**”), we (the folks at Automattic) process Personal Data on behalf of the users of those services (“**You**” or “**User**”), 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.

“Data Protection Laws” means any and all privacy, security and data protection laws and regulations that apply to the Personal Data processed by processor under the Agreement, including, as applicable, the GDPR, Member State laws implementing the GDPR, and the California Consumer Privacy Act of 2018, as amended.

“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.

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.

Please see below to determine which entity your Agreement is with, which depends on where you reside and which Services (as defined in the Terms of Service) you use. We use the term “Designated Countries” to refer to Australia, Canada, Japan, Mexico, New Zealand, Russia, and all countries located in Europe (including the UK and ROI).

### All Automattic Services (except WooCommerce)

- If you reside outside of the Designated Countries: Automattic Inc.
- If you reside in the Designated Countries: Aut O’Matic A8C Ireland Ltd.

### WooCommerce Services

*WooCommerce Services includes WooCommerce, WooCommerce Payments, WooCommerce Shipping, MailPoet, and any products or services purchased from WooCommerce.com.*

- If you reside outside of the Designated Countries: WooCommerce, Inc.
- If you reside in the Designated Countries: WooCommerce Ireland Ltd.

Each of the above referred to as “**Automattic**” or “**we**” in this Addendum.

## 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.** Automattic will not: (a) collect, retain, use, disclose or otherwise process the Controller Data for any purpose other than as necessary for the specific purpose of performing the services on behalf of the User; (b) collect, retain, use or disclose the Controller Data for a commercial purpose other

---

<sup>1</sup> If you use our Crowdsignal service, the Crowdsignal Terms and Conditions at <https://crowdsignal.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.

than providing the services on behalf of the User; or (c) sell the Controller Data.

- 2.3.** 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.

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.

- 2.4.** 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 agreement. Automattic will immediately inform the User if, in Automattic's opinion, an instruction from the User infringes applicable data protection law.
- 2.5.** 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.
- 2.6.** User agrees that Automattic may depersonalise the Controller Data or aggregate data in a way which does not permit the identification of a natural person, as well as 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 depersonalised or aggregated as above-mentioned are no longer classified as Controller Data in terms of this Addendum and that Automattic is instructed by User to depersonalise Controller Data in accordance with this clause.
- 2.7.** Automattic has the right to collect, use, and disclose any User data ("**User Data**") which is distinct from Controller Data in accordance with the Automattic privacy policy, which is available at <https://automattic.com/privacy/>. User Data includes 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 User Data is independent of the services that Automattic provides directly to the User for the User's website, and is not subject to this Addendum.
- 2.8.** 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 shall secure Controller Data in accordance with requirements under Data Protection Law. 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 **Appendix 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. Sub-processors

- 5.1. The User hereby authorizes Automattic to engage sub-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 sub-processors currently engaged by Aut O'Mattic Ltd. (Ireland) include its affiliate companies Automattic Inc. (US) and Pressable Inc. (US). For Users whose Agreement is with WooCommerce Ireland Ltd., the sub-processors currently engaged by WooCommerce Ireland Ltd., include its affiliate companies WooCommerce, Inc. and Automattic Inc. 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 make available to the User the current list of sub-processors at the following link: <https://automattic.com/subprocessor-list/>. User should check this website regularly for updates. Through this link, Automattic shall provide notice to the User of any intended changes concerning the addition or replacement of sub-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. Insofar as the User does not object within 14 days after the notification date, 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.

The agreement between Automattic and sub-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 sub-processor. In case Automattic engages a sub-processor outside of the European Economic Area, the User hereby instructs and authorises Automattic to conclude an agreement with another

processor on behalf of the User based on the Standard Contractual Clauses (as defined below) for the transfer of personal data to processors in third countries. As the case may be, where the Controller 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 sub-processor it engages is bound by the Standard Contractual Clauses (processor to processor Standard Contractual Clauses). 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.

**5.3.** Automattic shall monitor the technical and organisational measures taken by the sub-processors.

## **6. Support obligations of Automattic**

**6.1.** Automattic shall provide assistance to the User pursuant to its obligations under Article 28 GDPR.

**6.2.** 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.

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

- a) 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;
- b) the likely consequences of the breach of Controller Data;
- c) the measures taken or proposed by Automattic to remedy the breach of Controller Data and, where appropriate, measures to mitigate their potential adverse effects.

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

**6.5.** Automattic will take appropriate steps to promptly remediate the cause of any Security Incident and will reasonably cooperate with the User with respect to the investigation and remediation of such incident, including providing such assistance as required to enable User 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 User from curing an alleged violation of Data Protection Law.

## **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”).

**9. Standard Contractual Clauses Transfers**

As the case may be, the Controller 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, the Processor 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 Controller Data.

“**Standard Contractual Clauses**” mean the standard contractual clauses for the transfer of personal data to processors in third countries according to Decision (EU) 2021/914of the EU Commission of 4 June 2021.

<b>USER</b>	<b>AUTOMATTIC</b>
User Legal Name: _____  _____	<p>DocuSigned by: <i>Paul Sieminski</i></p> <hr/>
Signatory Name: _____	D9671DA172AD49E... Signatory Name: Paul Sieminski
Title: _____	Title: Chief Legal Officer of Automattic Inc. and WooCommerce, Inc.; Director of Aut O’Mattic A8C Ireland Ltd. and WooCommerce Ireland Ltd.
Date: _____	Date: September 27, 2021

## Appendix 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 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 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 Controller Data due to power supply failure or line interference, which may include fire protection and warning measures, emergency

power generators, and data recovery procedures.

## Appendix 2: Standard Contractual Clauses (processors)

Controller to Processor

### SECTION I

#### Clause 1

##### Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) <sup>(2)</sup> for the transfer of data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')
- have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### Clause 2

##### Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

---

<sup>2</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ([OJ L 295, 21.11.2018, p. 39](#)), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.



**Clause 3**

**Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4**

**Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

**Clause 7 – Optional**

**Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **SECTION II – OBLIGATIONS OF THE PARTIES**

### ***Clause 8***

#### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

#### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union <sup>(3)</sup> (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

---

<sup>3</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### **Clause 9**

#### **Use of sub-processors**

- (a) **GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 7 days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. <sup>(4)</sup> The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business

---

<sup>4</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### ***Clause 10***

#### **Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

### ***Clause 11***

#### **Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body<sup>5</sup> at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

---

<sup>5</sup> The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

### **Clause 12**

#### **Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13**

#### **Supervision**

(a) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses

in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### ***Clause 14***

##### **Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
- (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards <sup>(6)</sup>;
- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

---

<sup>6</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

### **Clause 15**

#### **Obligations of the data importer in case of access by public authorities**

##### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

##### **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it



remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS**

##### ***Clause 16***

##### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal

framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17**

**Governing law**

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 Ireland (*specify Member State*).

**Clause 18**

**Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland (*specify Member State*).
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

**EXPLANATORY NOTE:**

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

**ANNEX I**

**A. LIST OF PARTIES**

**Data exporter(s):** *[Identity and contact details of the data exporter(s), including any contact person with responsibility for data protection]*

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Contact person's name, position and contact details: \_\_\_\_\_

\_\_\_\_\_

Activities relevant to the data transferred under these Clauses:

Data exporter's use of data importer's services and data exporter's customers' websites and services.

Signature and date: \_\_\_\_\_

Role (controller)

**Data importer(s):** *[Identity and contact details of the data importer(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

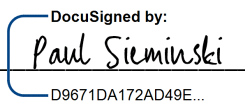
Name: Automattic

Address: 60 29th St, #343 San Francisco, CA 94110, United States

Contact person's name, position and contact details: Paul Sieminski; Chief Legal Officer of Automattic Inc. and WooCommerce, Inc.; Director of Aut O'Mattic A8C Ireland Ltd. and WooCommerce Ireland Ltd.; [privacypolicyupdates@automattic.com](mailto:privacypolicyupdates@automattic.com)

Activities relevant to the data transferred under these Clauses:

The data processing provided for by these standard contractual clauses is executed for the purpose of providing the services described in the Terms of Service.

Signature and date:  \_\_\_\_\_ September 27, 2021

Role (processor)

## **B. DESCRIPTION OF TRANSFER**

### Categories of data subjects whose personal data is transferred

End-users who use a customer of Automattic's website or service, which may include those customers' customers, subscribers, followers, employees or other administrative users and who are located in the Designated Countries; data subjects discussed in the contents of User's websites.

### Categories of personal data transferred

The type of data processed by data importer depends on the services and features that the data exporter uses, and may include personal data contained in content (text and media); username and credentials, such as password hashes; 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 by data exporter to a website, such as contact form submissions.

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).

Continuous

### Nature of the processing

collection, use, organisation, 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 Terms of Service.

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 Terms of Service, Privacy Policy, and Privacy Notice.

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

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

For Users whose Agreement is with Aut O'Mattic Ltd. (Ireland), the sub-processors currently engaged by Aut O'Mattic Ltd. (Ireland) include its affiliate companies Automattic Inc. (US) and Pressable Inc. (US) - the above categories and data subjects.

For Users whose Agreement is with WooCommerce Ireland Ltd., the sub-processors currently engaged by WooCommerce Ireland Ltd., include its affiliate companies WooCommerce, Inc. and Automattic Inc - the above categories and data subjects.

List of Subprocessors can be seen here: <https://automattic.com/subprocessor-list/>

## **C. COMPETENT SUPERVISORY AUTHORITY**

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

Data Protection Commission (Ireland)

## ANNEX II

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

#### EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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 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 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 Controller Data due to power supply failure or line interference, which may include fire protection and warning measures, emergency power generators, and data recovery procedures.