SITEGROUND DATA PROCESSING AGREEMENT

This Data Processing Agreement (this “DPA”) is entered between SiteGround Spain S.L. (“SiteGround”, “we”) and Customer (“Customer”, “you”), together referred as “The Parties”. This agreement (“DPA”) is part of the Terms of Service, Privacy Policy and other relevant policies available here. Customer agreeing to these terms enters in this DPA on their own behalf to the extent required under applicable Data Protection Regulations and Laws and to the extent SiteGround processes Customer Data as instructed by the Controller (as defined in the Section 1).

In the course of providing the Services to the Customer SiteGround may Process Customer Data on behalf of the Customer. The Parties agree to comply with the following provisions with respect to any Customer Data, each acting reasonably and in good faith.

1. Definitions.

Unless otherwise defined in this DPA, all capitalized terms have the meanings outlined below:

“Agreement” means the Terms of Service and other relevant policies announced on our website, together with your Order for the purchase of Services and the Order confirmation sent by SiteGround.

“Order” means any Customer’s order for purchase of the respective services.

“Site” means the SiteGround website and all services we offer through our website.

“Services” means any hosting services we offer and the Customer has purchased that could involve processing of Personal Data by SiteGround.

“Partner” means any entity that directly or indirectly controls, is controlled by, or is under common control with the SiteGround subject entity. “Control,” for the purpose of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Additional Products” means any features, products, software, programs, addons, plugins, scripts, tools or any other third-party software or content that are not part of the Services but that may be accessible via the SiteGround User Area or the Control Panel, installed by the Customer or otherwise for the usage of the Services.

“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 customer data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Controller” means the natural person or the legal entity which, alone or jointly with others, determines the purposes and means of the processing of customer data;

“Customer Data” means any "Personal Data" that is provided to SiteGround by, or on behalf of the Customer through their use of the Services and that is stored in the Customer’s account (for avoidance

of doubt Personal Data part of the Customer's order for purchase of the respective service shall not be treated as Customer Data). Customer Data may include, but is not limited to, customer data within the meaning set in the GDPR.

"Personal Data" has the meaning as given in Article 4 of GDPR.

"Data Protection Regulations and Laws" means all regulations and laws, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Customer Data under this DPA.

"Data Subject" means the identified or identifiable person to whom the Customer Data relates.

"Effective date" means, as applicable:

1. 25th May 2018, if the Customer has executed Order(s) and accepted the Agreements or the Parties have otherwise agreed to this DPA in respect of the applicable Agreement prior to or on such date; or
2. the date on which the Customer clicked to accept the Agreement or the Parties otherwise agreed to this DPA in respect of the applicable Agreement, if such date is after 25th May 2018.

"Processing" has the meaning as given in Article 4 of GDPR.

"Processor" means the entity which processes Customer Data on behalf of the Controller.

"SiteGround" means the SiteGround entity which is a party to this DPA, as specified in the section, a company incorporated in Kingdom of Spain (registration number CIF: B87194171), with address: Calle de Prim 19, 28004 Madrid, Spain.

"SiteGround Group of Companies" means SiteGround and its related parties engaged in the Processing of Customer Data:

- SG Hosting Inc. registered and existing under the laws of Delaware, USA, with address: 901 N. Pitt St, Suite 325, Alexandria 22314 VA, USA,
- SiteGround Spain S.L. registered and existing under the laws of the Kingdom of Spain (registration number CIF: B87194171), with address: Calle de Prim 19, 28004 Madrid, Spain
- SiteGround Italia Srl. registered and existing under the laws of Italy, VAT number and tax code no. 09659420963, registered in the Milan Companies Register, Italy, with address: Via Agnello 8, Milan 20121, Italy,
- SiteGround Hosting Ltd. registered in England and Wales (registration number 09348602), with address: 3rd Floor, 11-12 St James' Square, London, SW1Y 4LB
- SiteGround Hosting EOOD, registered in Bulgaria with UIC 204181297 and address: 8 Racho Petkov Kazandziata str., Sofia, Bulgaria.

"Standard Contractual Clauses" or "SCCs" means the standard data protection clauses for the transfer of Customer Data, as described in Article 46, p.2, c) of the GDPR, Appendix 1 to this DPA.

"Sub-processor" means any Processor engaged by SiteGround or a member of the SiteGround Group.

"Supervisory Authority" means an independent public authority, which is established in Kingdom of Spain within the territory of the EU Member State pursuant to the GDPR.

“Term” means the period from the Effective Date until the end of SiteGround's provisioning of the Services under the applicable Agreement, including, if applicable, any period during which the Services may have been suspended and any post-termination period (namely 60 calendar days) during which SiteGround may continue providing Services for transitional purposes.

“Data Protection Losses” means all liabilities, including:

1. costs (including legal costs);
2. claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (whether material or non-material, and including for emotional distress);
3. to the extent permitted by Applicable Law:
    1. administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Data Protection Supervisory Authority or any other relevant Regulatory Authority;
    2. compensation to a Data Subject ordered by a Data Protection Supervisory Authority;
    3. the reasonable costs of compliance with investigations by a Data Protection Supervisory Authority or any other relevant Regulatory Authority; and
4. the costs of loading Customer Data and replacement of Customer materials and equipment, to the extent that the same are lost or damaged, and any loss or corruption of Customer Data including the cost of rectification or restoration of Customer Data;

“Notification Email Address” means the email address specified by the Customer in the My Detail section in the User Area to receive certain notifications from SiteGround.

2. Data Processing.

2.1. Scope

This DPA applies where and only to the extent that SiteGround processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom (referred herein as "Customer Data").

If the Customer agreeing to this DPA is already a Customer, this DPA forms part of the Agreement, Privacy Policy and other relevant policies and documents announced on our website In such case, the SiteGround entity shall be considered as a party to this DPA.

This DPA is effective only for the Customer account it was agreed for. If the Customer owns multiple accounts, a DPA will be contracted for each individual account separately.

This DPA shall be valid and legally binding only for the physical/legal entity stated in the account in the User Area and only for the Services purchased directly from SiteGround within the respective account.

If the Customer entity agreeing to this DPA is neither a party to an Order nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

This DPA including its appendixes except the clauses in the Privacy Policy will be effective and replace any terms previously applicable to privacy, data processing and/or data security.

2.2. Compliance with Laws.

If European Union Data Protection Laws apply to this DPA, each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Data.

2.3. Subject Matter and Details of the Data Processing

2.3.1 Subject Matter

SiteGround will process Customer Data as necessary for the provisioning of the Services, related technical support and other inquiries pursuant to the Agreement and as further instructed by Customer in its use of the Services.

2.3.2. Duration of processing

Subject to Section 11, the duration of data processing shall be the Term designated under the Order and the applicable Agreement.

2.3.3. Nature and Purpose of the Processing

SiteGround will process Customer Data for the purposes of providing the Services and related technical support to the Customer in accordance with the Agreement, this DPA and other relevant policies.

2.3.4. Categories of Data Subjects

Customer may submit Customer Data in the course of its use of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of the Customer (who are natural persons and legal entities);
- Employees or contact persons of the Customer's prospects, customers, business partners and vendors;
- Employees, agents, advisors, freelancers of the Customer (who are natural persons);
- Customer's Users authorized by the Customer to use the Services;
- Individuals who transmit data via the Services, including individuals collaborating and communicating with the Customer or Customer's end users;
- Individuals whose data is provided to SiteGround via the Services by or at the direction of the Customer or by the Customer's end users.

2.3.5. Categories of Personal Data

Customer may submit Customer Data in the course of its use of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Personal Data:

- Name
- Address
- Email address
- Any personal data relating to individuals

2.4. Roles of the Parties

The parties acknowledge and agree that:

1. SiteGround is a processor of the Customer Data under the European Data Protection Legislation;
2. Customer is a controller or processor, as applicable, of the Customer Data under the European Data Protection Legislation; and has obtained all consents and rights necessary under Data Protection Laws for SiteGround to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

2.5. Instructions for Data Processing.

SiteGround shall process Customer Data in accordance with this DPA, which is the Customer's complete and final instructions to SiteGround in relation to processing of Customer Data. Processing outside the scope of this DPA (if any) shall require prior written agreement between SiteGround and Customer on additional instructions for processing. By entering into this DPA, Customer instructs SiteGround to process Customer data only in accordance with applicable law:

1. to provide the Services and related technical and other support;
2. as initiated by the Customer and end users in their usage of the Services;
3. as specified in the Agreement, Terms of Service, Privacy Policy and other relevant policies governing the provision of the Services and related technical and other support.

2.6. Access or Use.

SiteGround shall not access or use Customer Data, except as necessary to provide the Services and related technical support to the Customer in accordance with the DPA, the Agreement and other relevant policies.

2.6.1. Customer's Processing.

The Customer shall, in their use of the Services, Process their Data in accordance with the requirements of Data Protection Laws and Regulations applicable to it. The Customer shall have sole responsibility for the accuracy, quality, and legality of their Data and the means by which the Customer acquired this Data.

2.6.2. SiteGround's Processing of Customer Data.

SiteGround shall only Process Customer Data on behalf of and in accordance with the Customer's documented instructions for the following purposes:

1. Processing to provide the Services and related technical support in accordance with this DPA and applicable Order(s);
2. Processing initiated by Users in their usage of the Services;
3. Processing necessary to maintain and improve the Services.

2.6.3. SiteGround's Compliance with Instructions.

As from the Effective Date SiteGround shall comply with the described instructions above in the Section Customer's Instructions, including with regard t o data transfers, unless EU or EU Member State law to which SiteGround is subject requires other processing of Customer Data by SiteGround, in which case

SiteGround shall inform the Customer (unless that law prohibits SiteGround from doing so on important grounds of public interest) via the Site or the Notification Email Address.

Customer Data may be accessed and processed by SiteGround, Authorized Users and Sub-processors to fulfill the obligations under this DPA and the respective Agreement or to provide certain services on behalf of SiteGround. Such processing will comply with the measures outlined in Sections 3, Section 7 and Annex 2 Security Measures.

2.7. Rights of the Data Subjects.

2.7.1. Access, Rectification, Restricted Processing, Portability.

During the applicable Term, SiteGround shall, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict processing of Customer Data, including via deletion of all or some of the Customer Data under their account or deletion of the whole account as described in Section 2.6. (Return and Deletion of customer data), and via export of Customer Data.

2.7.2. Data Subject Requests.

2.7.2.1. Customer's Responsibility for Requests.

If during the applicable Term, SiteGround receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"), SiteGround shall advise the Data Subject to submit his/her request to the Customer, and the Customer shall be responsible for responding to any such request including, where necessary, by using the functionality of the Services. SiteGround shall, to the extent legally permitted, take commercially reasonable steps to notify the Customer about such requests.

2.7.2.2. SiteGround Data Subject Request Assistance.

Taking into account the nature of the Processing, Customer agrees that SiteGround shall provide appropriate technical and organizational assistance, insofar as this is possible, for the fulfillment of Customer's obligation to respond to requests by Data Subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

(a) providing documentation resources in the form of tutorials and knowledge base articles, functionality and/or controls in the Control Panel that Customer may elect to use to properly configure the Services and use the Services in secure manner.

(b) providing features, functionalities and/or controls in the Control Panel that Customer may elect to use to retrieve, correct or delete the Customer Data from the Services.

(c) complying with the commitments set out in this DPA.

(d) To the extent Customer, in their use of the Services, does not have the ability to address a Data Subject Request, SiteGround shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent SiteGround is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from SiteGround's provisioning of such assistance.

The Customer shall cover SiteGround's reasonable costs of providing assistance in section 2.7.2.2.

2.8. Return and Deletion of customer data.

SiteGround shall enable Customer to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services and the features as per the respective Order. If the Customer uses the Services to retrieve or delete Customer Data and the Customer Data cannot be recovered, this shall constitute an instruction to SiteGround to delete the relevant Customer Data archived on backup systems in accordance with applicable law and within maximum period of 60 calendar days.

Deactivation of the Services or expiry of the applicable Term shall constitute an instruction to SiteGround to delete the Customer Data and the relevant Customer Data archived on backup systems within maximum period of 60 calendar days.

Nothing in this Section 2.8 varies or modifies any obligation of SiteGround to retain some or all Customer Data as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or a court order).

2.9. Disclosure.

SiteGround shall not disclose Customer Data to any government, law enforcement agencies and other authorities, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or a court order).

2.10. SiteGround's Personnel.

SiteGround restricts its personnel from processing Customer Data without authorisation by SiteGround. Access to Customer Data is limited to those personnel performing a role and responsibilities in accordance with the Agreement.

SiteGround imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. SiteGround ensures that these confidentiality obligations survive the termination of the personnel engagement.

2.11. Data Protection Officer.

Member/s of the SiteGround Group have appointed a Data Protection Officer for the purposes of this DPA and Privacy Policy, who be reached at privacy@siteground.com.

3. Sub-processors.

3.1. Consent to Sub-processor Engagement/Appointment of Sub-processors

The Customer acknowledges and agrees that:

(a) SiteGround Partners may be retained as Sub-processors; and

(b) SiteGround and SiteGround Partners respectively may engage Sub-processors in connection with the provisioning of the Services. SiteGround has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processors. If Customer has entered into Standard Contractual Clauses (Appendix 1) as described in Section 5 (Transfers of Data Out of the EEA), the above authorizations shall constitute Customer's prior

written consent to the subcontracting by SiteGround of the processing of Customer Data if such consent is required under the Standard Contractual Clauses.

3.2. Information about sub-processors/ Notification of new Sub-processors.

3.2.1. SiteGround will share information about you with Sub-processors such as the SiteGround Group of companies who are engaged with provisioning of Services subject to your Agreement and who are based within the territory of the European Union and United States, Sub-processor/processors who are engaged with provisioning Services subject to your Agreement and who are based within the territory of the European Union and United States, Data Center service providers who are based within the territory of European Union, United States and Singapore. These Sub-processors shall process the provided data under instructions of SiteGround and in compliance with our Privacy Policy and this DPA. We do not authorize Sub-processors to retain, share, store or use your personally identifiable information for any secondary purposes.

3.2.2. When a new Third Party Sub-processor is engaged to process any Customer Data in connection with the provisioning of the applicable Services during the applicable Term of this DPA, SiteGround shall inform the Customer of this engagement, including the category and location of the relevant sub-processor and the activities it shall perform, at least 10 calendar days before authorizing the new Third Party Sub-processor either by sending an email to the Notification Email Address or via the User Area.

3.3. Requirements for Sub-processor Engagement.

When engaging any Sub-processor, SiteGround shall:

(a) ensure via a written contract that:

(i) the Sub-processor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Data Processing Amendment) and any Standard Contractual Clauses entered into or Alternative Transfer Solution adopted by SiteGround as described in Section 5 (Transfers of Data Out of the EEA); and

(ii) if the GDPR applies to the processing of Customer customer data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Data Processing Amendment, are imposed on the Sub-processor; and

(b) remain fully liable for all obligations subcontracted to it, and all acts and omissions of, the Sub-processor.

3.4. Objection Right for New sub-processors.

3.4.1. Customer may object to any new Third Party Sub-processor by terminating the applicable Agreement immediately upon written notice to SiteGround, on condition that Customer provides such notice within 10 calendar days of being informed of the engagement of the sub-processor. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Sub-processor.

3.4.2. SiteGround shall refund Customer any prepaid fees covering the remainder of the term of such Order(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on the Customer.

4. Impact Assessments, Consultations. Storage.

4.1. Impact Assessments and Consultations.

Upon Customer's request, SiteGround shall provide the Customer with reasonable cooperation and assistance needed to fulfil the Customer's obligation under the GDPR to carry out a data protection impact assessment related to the Customer's use of Services, to the extent the Customer does not otherwise have access to the relevant information, and to the extent that such information is available to SiteGround. SiteGround shall provide reasonable assistance to the Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this DPA, to the extent required under the GDPR.

5. Transfers Out of the EEA.

5.1. Data Center and storage

SiteGround stores and process Customer Data in Data Centers located inside and outside the European Union. Information about our Data Center locations is available on: https://www.siteground.com/datacenters and SiteGround reserves the right to update it from time to time.

The Customer may specify the Data center location where their Customer Data will be stored. The Customer agrees that SiteGround may change the locations of the Data Centers and move Customer Data to another Data Center. SiteGround shall inform the Customer at least 10 calendar days before moving Customer Data to a new Data Center either by sending an email to the Notification Email Address or via the User Area. If the change of the Data Center results in storing the Customer Data under a different jurisdiction, the Customer may object to such change by terminating the Agreement immediately and upon written notice to SiteGround, on condition that the Customer provides such notice within 10 calendar days of being informed of the change of the Data Center.

The Customer can move their account and Customer Data to another Data Center location at any time, provided that the functionality of the Services allows it and in exchange of additional fees. Once the Customer has made their choice and specified a Data Center location within the European Union, SiteGround will not store Customer Data outside the borders of European Union except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or a court order).

5.2. Processing Locations

To the extend the Customer has specified a Data Center outside the European Economic Area and to the extend SiteGround provides the Services and related technical and other support, the Customer agrees that SiteGround may, subject to Section 5, access and process Customer Data in EEA, United States and any other countries where SiteGround and/or its Partners and Sub-processors have Data Centers, facilities or maintain data processing operations. If the storage and/or processing of Customer Data involves processing of Customer Data outside of the EEA, and the European Data Protection Legislation applies, the Customer agrees that SiteGround reasonably requires the Customer to enter into Model Contract Clauses in respect to such transfers in accordance with Section 5.2 and Appendix 1 and the Customer agrees to do so..

5.3. Transfer Mechanism

To the extent SiteGround processes or transfers (directly or via onward transfer) Customer Data under this DPA from the European Union, the European Economic Area and/or their member states and Switzerland in or to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws of the foregoing territories, the parties agree that:

1. The Standard Contractual Clauses (Appendix 1) will apply to Customer Data that is transferred.
2. SiteGround shall be deemed to provide appropriate safeguards to protect Customer Data by virtue of making available Standard Contractual Clauses (Appendix 1) as a transfer mechanism.
3. The Customer hereby authorises any transfer or access to Customer Data from such destinations outside the European Economic Area subject to any of the measures above;

6. Processing records.

The Customer acknowledges that SiteGround is required under the GDPR to:

(a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which SiteGround is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and

(b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer data, the Customer shall, where requested, provide such information to SiteGround via the Site or other means provided by SiteGround, and shall use the Site or such other means to ensure that all provided information is kept accurate and up-to-date.

7. Security Responsibilities of SiteGround.

7.1. SiteGround shall implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). As described in Appendix 2, the Security Measures include measures to provide encrypted transmission of customer data outside the Service environment; to help ensure ongoing confidentiality, integrity, availability and resilience of SiteGround's systems and services; to help restore timely access to Customer Data from an available backup copy, provided either by SiteGround Backup Services or Customer's own backup copy following an incident; and for regular testing of effectiveness. SiteGround may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

7.2. Customer's Security Responsibilities and Assessment.

The Customer agrees that, without prejudice to SiteGround's obligations under Section 7. (Security Responsibilities of SiteGround) and other relevant Sections in this DPA:

1. The Customer is solely responsible for their use of the Services, including:
    1. making appropriate use of the Services to ensure a level of security suitable to the risk in respect of the Customer Data;

2. securing the account authentication credentials, systems, and devices the Customer uses to access the Services;
3. ensuring that all programs, scripts, addons, plugins and other software installed on the account are secure and their utilization does not impose any security risk in respect to the Customer Data and the account itself;
4. securing all installed programs, scripts, addons, plugins and other software, their configuration and their regular maintenance;
5. any content of the account;
6. any actions and activity on the account; and
7. backing up their Customer Data; and

2. SiteGround has no obligation to protect Customer Data that the Customer chooses to store or transfer outside of SiteGround's and its Sub - processors' systems (for example, offline or on-premise storage), or to protect Customer Data by implementing or maintaining Additional Security Controls except to the extent the Customer has opted to use them.
3. The Customer is solely responsible for reviewing the documentation and evaluating whether the Services, the Security Measures, SiteGround's commitments under this Section and the following meet the Customer's needs, including any security obligations of the Customer under the European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable.
4. The Customer acknowledges and agrees that (taking into account the costs of implementation and the nature, scope, context and purpose of processing of Customer data as well as the risks to individuals) the Security Measures implemented and maintained by SiteGround as set out in Section 7.1. provide the needed level of security appropriate to the risk in respect to the Customer Data.
5. It is the Customer's responsibility to backup Customer Data and all data and consent stored within the account in order to prevent potential data loss.
    1. SiteGround Backup Services are provided "as-is" and are subject to all limitations of liability set out in the applicable Agreement.
    2. Even if the Customer purchases Backup Services, they agree that they will maintain their own set of backups independent of those that SiteGround maintains and that SiteGround's only obligation is to restore the account space to its operating condition. In the event of an incident, hardware or software failure or any incidental data corruption or loss, SiteGround may provide assistance but it is the Customer's sole obligation to restore the Customer Data.
    3. In the event of partial or full data loss or corruption and in case that the Customer is not satisfied with the outcome of the restore by the SiteGround Backup Services or SiteGround's backup copy is not recent or suitable for restore, it shall be the Customer's obligation to restore Customer Data, their files and any data within the account from Customer's own backup.

8. Review and Audits of compliance.

If the European Data Protection Legislation applies to the processing of Customer Data:

1. The Customer has the right to verify SiteGround's compliance with its obligations under this DPA, by conducting a review of documentation or an audit, including inspections, conducted by the Customer

or an independent auditor appointed by the Customer, by making a specific request to SiteGround in a written form to the address set in the respective Terms of Service.

2. SiteGround shall further provide written responses to all reasonable requests by the Customer and may charge a fee for any review or audit. SiteGround will provide details of any applicable fee in advance of any such audit and the Customer will be responsible for any fees charged by any auditor and any fees associated with executing an audit. The reports of any such audit will be made available to SiteGround without restrictions of the purposes for its further usage by SiteGround.
3. SiteGround may object and decline in writing to the Customer or an auditor appointed by the Customer to conduct any audit if the Customer or the auditor is, in SiteGround's reasonable opinion, not suitably qualified or independent, a competitor of SiteGround, or otherwise manifestly unsuitable.
4. If SiteGround declines to follow any instruction requested by the Customer or an auditor regarding a properly requested and scoped audit or inspection, the Customer is entitled to terminate this DPA and the Terms of Service.

Nothing in this Section 9 (Review and Audits of Compliance) varies or modifies any rights or obligations of Customer or SiteGround under any Model Contract Clauses entered into as described in Sections 5 (Transfers of Data Out of EEA).

9. Security Breach Notification.

9.1. SiteGround maintains security incident management policies and procedures and shall notify the Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Customer data transmitted, stored or otherwise Processed by SiteGround or its Sub-processors of which SiteGround becomes aware (a "Customer Data Incident"). SiteGround shall make reasonable efforts to identify the cause of such Customer Data Incident and take the steps as SiteGround deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within SiteGround's reasonable control. The obligations herein shall not apply to incidents that are caused by the Customer, Customer's usage of the Services, Customer's actions or activities or Customer's Users.

9.2. Notifications made pursuant to this section shall describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps SiteGround recommends the Customer takes to address the Data Incident.

9.3. Notification(s) of any Data Incident(s) shall be delivered to the Notification Email Address or, at SiteGround's discretion, by direct communication (for example, by phone call). The Customer is solely responsible for ensuring that the Notification Email Address and contact information is current and valid.

9.4. SiteGround shall not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to the Customer and fulfilling any third party notification obligations related to any Data Incident(s).

9.5. SiteGround's notification of or response to a Data Incident under this Section 10 shall not be construed as an acknowledgement by SiteGround of any fault or liability with respect to the Data Incident.

10. Liability and indemnity.

10.1. The Customer shall indemnify and keep indemnified SiteGround with respect to all data protection breaches and losses suffered or incurred by, arising from or in connection with:

(a) any non-compliance by the Customer with data protection laws and regulations;

(b) any breach by the Customer of its data protection obligations under this Agreement;

10.2. SiteGround shall be liable for data protection breaches and losses caused by processing of Customer Data only to the extent directly resulting from SiteGround's failure to comply with its obligations as Data Processor under Data Protections laws and Regulations.

11. Termination

This DPA will take effect from the Effective Date until the end of SiteGround's provisioning of the Services under the applicable Agreement, including, if applicable, any period during which the Services may have been suspended and any post-termination period (namely 60 calendar days) during which SiteGround may continue providing Services for transitional purposes ("Term"). The DPA will automatically expire upon deletion of all Customer Data by SiteGround.

12. Legal Effect.

To the extent of any conflict or inconsistency between the terms of this DPA and the remainder of the applicable Agreement related to the Processing of Customer Data, the terms of this DPA shall govern. Subject to the amendments if any in this DPA, such Agreement remains in full force and effect. For clarity, if the Customer has entered more than one Agreement, this DPA shall amend each of the Agreements separately.

Annex 1

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

The entity identified as "Customer" in the Data Processing Agreement

(the data exporter)

And

SiteGround Spain S.L.

(the data importer)

each a ‘party’; together ‘the parties’,

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) ‘the data exporter’ means the controller who transfers the personal data;

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

(d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue

the transfer or to lift the suspension;

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

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

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

Clause 5

Obligations of the data importer [1]

The data importer agrees and warrants:

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

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

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

(d) that it will promptly notify the data exporter about:

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

(ii) any accidental or unauthorised access; and

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

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

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

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

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

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

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

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

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

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

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

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

Clause 12

Obligation after the termination of personal data-processing services

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

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Appendix 1 to the Standard Contractual Clauses

Data exporter

The data exporter is the entity identified as "Customer" in the Data Processing Agreement

Data importer

The data importer is SiteGround Spain S.L.

Data subjects

The personal data concerns the categories of data subjects as defined in Section 2.3.4. in the Data Processing Agreement.

Categories of data

The personal data concerns the categories of data as defined in Section 2.3.5. in the Data Processing Agreement.

Processing operations

The processing operations are defined in Section 2 of the Data Processing Agreement.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. By purchasing Services from SiteGround and agreeing the Data Processing Agreement, the parties will be deemed to have accepted and executed this Appendix 2.

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

The technical and organisational security measures implemented by the data importer are as described in the Data Processing Agreement and Annex 2 Security Measures.

Annex 2

Security Measures

SiteGround implements and maintains appropriate technical and organizational Security Measures for the Processing of Personal Data, including the measures set out in this Appendix 2 to the Data Processing Agreement. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the particular Services ordered by Customer, may be specified in the Agreement.

SiteGround may update or modify these Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

The technical and organisational security measures implemented by SiteGround are in accordance with Clauses 4(c) and 5(c) of the Standard Contractual Clauses.

Personnel and Confidentiality

SiteGround shall take reasonable steps to ensure that no person shall be appointed by SiteGround to process Personal Data unless that person:

1. is competent and qualified to perform the specific tasks assigned to him by SiteGround;
2. has been authorised by SiteGround; and
3. has been instructed by SiteGround in the requirements relevant to the performance of the obligations of SiteGround under these Clauses, in particular the limited purpose of the data processing.

SiteGround personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. SiteGround conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, SiteGround's confidentiality and privacy policies. They are provided with training and personnel handling Customer Data are required to complete additional requirements appropriate to their role.

Physical Security

SiteGround uses geographically distributed data centers and stores all production data in physically secure data centers. SiteGround Sub-processor's production data centres employ measures to secure the access to data processing systems. They have an access system that controls access to the data center. This system permits only authorised personnel to have access to secure areas. The facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, CCTV monitoring, access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

The data center electrical power systems are designed to be redundant and maintainable without impact to continuous 24/7 operations. In most cases, a primary as well as an alternate power source is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries or diesel generators which are capable to provide emergency electrical power supply or reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions.

Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. SiteGround Sub-processor's production equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

System Access Control

SiteGround servers use a Linux based implementation customized for the Services. SiteGround employs a review process to increase the security of the operating systems used to provide the Services and enhance the security products in production environments.

SiteGround has, and maintains, a security policy for the personnel. SiteGround infrastructure, development and support personnel are responsible for the ongoing monitoring of SiteGround's security of the infrastructure, the review of the Services, and responding to security incidents.

SiteGround's internal access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process customer data, including personal data. SiteGround aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. SiteGround employs an access management system to control personnel access to production servers, and only provides access to authorized personnel. The following may, among other controls, be applied depending upon the particular Services ordered: authentication via passwords and/or two-factor authentication, SSH keys, authorization processes, change management processes, logical access to the data centers is restricted

and protected by firewall/VLAN and logging of access on several levels. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with SiteGround's internal data access policies.

Services Access Control

Customer and End Users must authenticate themselves via an authentication system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User.

The following may, among other controls, be applied depending upon the particular Services ordered: authentication via passwords and/or two-factor authentication, SSH keys, authorization processes, change management processes, and logging of access on several levels. Depending upon the particular Services ordered the following controls may also apply: unique identifiers are attributed to the responsible individual, revoke access mechanisms on consecutive failed login attempts and lockout time periods, password expiry and reset mechanisms, password complexity requirements.

Data Access Control

SiteGround stores data in a multi-tenant environment, meaning that multiple customers' deployments are stored on the same physical hardware. SiteGround uses logical isolation to segregate each Customer's data and logically separates each Customer's data from that of others. This provides the scale while rigorously preventing customers from accessing one another's data.

Customer is given control over specific controls for sharing access to the data to End Users for specific purposes in accordance with the functionality of the Services. Customer may choose to make use of these controls. SiteGround makes available certain logging capability.

Direct access to customer data is restricted and in case such is required access rights are established and enforced only to properly authorized staff in addition to the access control rules set forth in the previous Sections.

Transmission Control

Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media or exchanged within the data center.

For data in transit, SiteGround uses industry standard transport protocols such as SSL and TLS between Customer devices and SiteGround's Services and data centers, and within data centers themselves. Except as otherwise specified for the Services (including within the Order, the applicable Agreement or the User documentation of the Services), transmissions of data outside the Service environment are encrypted. Some functionalities of the Services may enable the Customer to choose unencrypted communications in their use of the Service. Customer is solely responsible for the results of its decision to use such unencrypted communications or transmissions.

Input Control

The Personal Data source is under the control of the Customer, and Personal Data integration into the system, is managed by secured file transfer, via web services or entered into the application from the Customer. As set forth in Section Transmission Control above, some functionalities of the Services

permit Customers to use unencrypted file transfer protocols. In such cases, Customer is solely responsible for its decision to use such unencrypted field transfer protocols.

The Services will not introduce any viruses to Customer Data; however, the Services do not scan for viruses that could be included in attachments or other Personal Data uploaded into the Services by Customer. Any such uploaded attachments will not be executed in the Services and therefore will not damage or compromise the Service.

Network Control

SiteGround blocks unauthorized traffic to and within the data centers using a variety of technologies such as firewalls, NATs, partitioned Local Area Networks and physical separation of back-end servers from public-facing interfaces.

SiteGround employs multiple layers of network devices and intrusion detection to protect its external attack surface. SiteGround considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

SiteGround and authorized personnel will monitor the Services for unauthorised intrusions using network-based intrusion detection mechanisms. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. SIteGround's intrusion detection involves tightly controlling the network communication attack surface through preventative measures such as firewalls, employing intelligent detection controls at data entry points and employing technologies that automatically remedy certain dangerous situations.

Incident Response

SiteGround maintains security incident management policies and procedures and monitors a variety of communication channels for security incidents. SiteGround personnel will react promptly to known incidents and will promptly notify Customer in the event SiteGround becomes aware of an actual or reasonably suspected unauthorised disclosure of Personal Data.

System Logs

SiteGround ensures that processing systems used to store Customer Data log information to their respective system log facility. Log entries are maintained in case there is suspicion of inappropriate access and an analysis is required. Logging is kept securely to prevent tampering.

Reliability and Backup

For the Services, SiteGround ensures that backups are taken on a regular basis. Backups are secured using a combination of technical and physical controls.

SiteGround ensures that the systems where Customer Data is stored have a disaster recovery facility and are governed under disaster recovery plan. In the event production facilities are to be rendered unavailable, SiteGround will execute recovery plans to restore operation in timely manner. SiteGround has designed and regularly plans and tests its disaster recovery plans.

Data destruction

When customers delete data or leave the Service, SiteGround ensures the data is deleted as per the terms in the applicable Agreement. For certain disks SiteGround follows strict rigorous standards that call for overwriting storage resources before reuse, as well as physically disposing of decommissioned hardware. SiteGround Sub-processor's production data centres employs strict procedures for reuse, redeployment, data destruction and decommission of disks and hardware.

Subprocessor Security

Before onboarding Sub-processors, SiteGround conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. The Sub-processor is required to enter into appropriate security, confidentiality and privacy contract terms.

System Changes and Enhancements

SiteGround may enhance and implement changes in the Services during the term of the Agreement. Security controls, procedures, policies and features may change or be added. SiteGround will provide security controls that deliver a level of security protection that is not materially lower than that provided as of the Effective Date.

Annex 3: List of Sub-processors

Available upon request.

CLOSE WINDOW