Kinsta Inc. Data Processing Addendum

Updated on: July 15, 2019

1. Introduction and Scope

1. This Data Processing Addendum ("DPA") is a part of the Terms of Service, Privacy Policy, and other relevant policies and agreements located on Kinsta's website at https://kinsta.com/legal/ (collectively, the "Agreement"). If there is a conflict between this DPA and any other provisions in the Agreement (other than this DPA), then the provisions of this DPA shall control.

2. This DPA is a binding agreement between Kinsta and its Clients, but only to the extent that (a) Kinsta Processes Client Personal Data (defined below) for or on behalf of the Client pursuant to the Agreement (b) and the Data Protection Laws apply to such Client Personal Data. By using our Services in any way, you are agreeing to the terms of this DPA.

2. Definitions

Capitalized terms which are not defined herein shall have the meaning provided elsewhere in the Agreement. In addition, the following defined terms apply solely with respect to this DPA.

1. "**Controller**", "**Processor**", "**Data Subject**", "**Processing**", "**Personal Data**", and "**Personal Data Breach**" shall have the meanings ascribed to them in Data Protection Laws.

2. "**Client Personal Data**" means any Personal Data subject to the Data Protection Laws that Client provides, transfers, or makes accessible to Kinsta in connection with the Services.

3. "**Data Protection Laws**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and any similar or related implementing legislation by European Union or European Economic Area member states, the United Kingdom, or Switzerland.

3. Roles of the Parties

1. Client is the Controller and Kinsta is the Processor with respect to Client Personal Data. Kinsta shall only Process Client Personal Data in accordance with Client's documented instructions, which include the provisions of the Agreement, unless otherwise required to comply with any Data Protection Laws. We will inform you if, in our opinion, your instructions violate the Data Protection Laws.

2. Client and Kinsta shall comply with the Data Protection Laws. Client shall obtain any required authorizations, consents, releases, or permissions, and provide all required privacy notices, regarding the Client Personal Data. For the avoidance of doubt, Client shall have sole responsibility for the accuracy, quality, and legality of all Client

Personal Data and the bases on which it is collected from the Data Subject.

4. Nature, Purpose, and Duration of Processing

1. Kinsta will Process Client Personal Data as necessary to perform the Services - which is generally limited to passive hosting of Client websites - or to protect Kinsta's legal rights, for the duration of the Agreement, unless otherwise agreed upon in writing. Client's transfer of Client Personal Data to Kinsta in connection with the Services is determined and controlled by Client in its sole discretion.

2. Kinsta may Process the following categories of Client Personal Data: any Personal Data collected, used, or otherwise Processed from End User Data Subjects in connection with Client Websites.

3. Kinsta may Process Client Personal Data from the following categories of Data Subjects: End Users of Client Websites.

5. Cross-border Transfers

1. You choose the [Google Cloud Platform data center(s)](#) where your websites will be hosted. You acknowledge, agree, and understand that (a) all of your Client Personal Data will be automatically transferred and stored in the Google data center you choose, and (b) Client Personal Data may be transferred from the European Economic Area, the United Kingdom, or Switzerland to the country where the Google data center is located, depending on your choice.

2. Kinsta and Google have agreed to the [Google Cloud Platform Data Processing and Security Terms and EU Model Contract Clauses](). For additional information, see Google's commitments regarding cross-border transfers in the "International Data Transfer" section here: https://cloud.google.com/security/gdpr/.

6. Sub-processors

1. Kinsta engages third-party subcontractors that Process Client Personal Data ("**Sub-processors**") for the purposes of providing the Services. A current list of Sub-processors is available below in Appendix A. Client authorizes Kinsta to engage these Sub-processors for the purpose of providing the Services.

2. Kinsta may update the list of Sub-processors in Appendix A from time to time, and such updates shall be the sole means of providing notice of Sub-processor changes to Client. Client is responsible for regularly checking and reviewing the list of Sub-processors in Appendix A. Client's failure to object in writing to a new Sub-processor within fourteen (14) days of Kinsta's posting of the new Sub-processor shall constitute Client's authorization of the new Sub-processor.

3. If Kinsta determines in its sole discretion that it cannot reasonably accommodate Client's timely objection to a Sub-processor, upon notice from Kinsta, Client may choose to terminate the Agreement pursuant to the termination provisions in the [Terms of Service](), which shall be Client's sole and exclusive remedy.

4. Kinsta shall impose obligations on its Sub-processors that are the same as or substantially equivalent to those set out in this DPA by way of written contract. Kinsta shall be liable to Client for the Sub-processors' performance of its data protection obligations with respect to Client Personal Data.

7. Security and Impact Assessments

1. Kinsta shall ensure that its personnel are subject to binding obligations of confidentiality with respect to Client Personal Data.

2. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, Kinsta shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

3. Taking into account the nature of Processing and the information available to Kinsta, Kinsta shall assist the Client in ensuring compliance with Client's obligations under the Data Protection Laws with respect to security, impact assessments, and consultations with supervisory authorities or regulators.

8. Personal Data Breach

1. Taking into account the nature of Processing and the information available to Kinsta, Kinsta shall assist the Client in ensuring

compliance with Client's obligations under the Data Protection Laws with respect to a Personal Data Breach.

2. In the event of a discovered Personal Data Breach, Kinsta shall provide prompt notice to Client's technical and account contacts using those means established for routine account-related communications.

3. Our notice shall include the following information to the extent it is reasonably available to Kinsta at the time of the notice, and Kinsta shall update its notice as additional information becomes reasonably available: (a) the dates and times of the Personal Data Breach; (b) the basic facts that underlie the discovery of the Personal Data Breach, or the decision to begin an investigation into a suspected Personal Data Breach, as applicable; (c) a description of the Client Personal Data involved in the Personal Data Breach, either specifically, or by reference to the data set(s), and (d) the measures planned or underway to remedy or mitigate the vulnerability giving rise to the Personal Data Breach.

9. Data Subject Requests

1. Taking into account the nature of the Processing, Kinsta shall assist Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests for exercising the Data Subject's rights under the Data Protection laws.

2. Kinsta will promptly notify Client if we receive a request from a Data Subject to invoke their rights with respect to Client Personal Data, unless otherwise prohibited by applicable law; and, except to the extent required by applicable law, we will not independently take any action in response to a request from a Data Subject without Client's prior written instruction.

10. Audit and Inspection

1. Subject to and conditioned on a written non-disclosure agreement, Kinsta shall provide Client with information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA.

2. Any on-site audits shall be (i) subject to and conditioned on reasonable advance written notice, not less than sixty (60) days, to Kinsta; (ii) subject to and conditioned on a written non-disclosure agreement and a detailed written audit plan reviewed and pre-approved by Kinsta; (iii) limited to once every three (3) calendar years; (iv) at Client's sole cost and expense; (v) limited in scope and purpose to evaluate a specifically identified suspected failure by Kinsta to comply with the provisions of this DPA and only after Client has exhausted all other reasonable means as determined by Kinsta; and (vi) in the presence of a Kinsta representative without unreasonably disrupting Kinsta's business operations.

11. Deletion or Return of Client Personal Data

Upon proper termination of the Agreement and at the written direction of the Client, Kinsta shall take reasonable measures to delete Client Personal Data or return Client Personal Data and copies thereof to the Client, subject to applicable laws requiring the continued storage of the Client Personal Data by Kinsta.

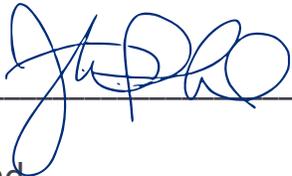Customer Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

Kinsta Inc. Signature: _____

Print Name: Jon Penland

Title: Director

Date: July 15, 2019

Appendix A

List of Sub-processors

- Google Cloud Platform: We use Google Cloud servers to host and secure Client Websites and store data related to Client Websites.
- Packet: We collect and analyze logs – that are necessary for operating our infrastructure – for security reasons on Packet servers.
- Intercom: We use Intercom to communicate with our customers and provide them support. Also, it is used to manage leads.
- Google Apps: We use Google/Google Apps to process email communication and manage online documents.
- Sendgrid: SendGrid is a cloud-based SMTP provider that we use to send transactional and marketing emails.
- KeyCDN: We use KeyCDN to power Kinsta CDN. If you enable Kinsta CDN on a website the website's static assets will be delivered by KeyCDN which will receive the IP addresses of website visitors.
- Slack: We use Slack for internal communication and collaboration.
- Stripe: We use Stripe to process Client payments.