Kinsta Inc. Data Processing Addendum

Updated on: July 7, 2023

***Note*: This is not the current version of this document and is provided for archival purposes. View the current version.**

1. Introduction and Scope

A. This Data Processing Addendum ("**DPA**") is an addendum to the Terms of Service ("**Terms**") and is part of the Agreement (as defined in the Terms). All provisions of the Terms, including its limitations of liability, apply to and are incorporated into this DPA. If there is a conflict between the provisions of this DPA and any provisions in the Terms, then the provisions of this DPA shall control.

B. **Updates to the DPA**. We may make changes to this DPA at any time in our sole discretion. We will provide email notice of any material changes to this DPA to the Company Owner (defined below). We may also post a notice of such changes in MyKinsta. Your continued use of our Services for more than 30 days following our email notification to the Company Owner will constitute your acceptance of our changes to this DPA. If you do not agree to any changes to this DPA, you may terminate your Account and the Agreement pursuant to Section 9 of the Terms.

2. Definitions

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

A. "**Controller**", "**Business**", "**Processor**", "**Service Provider**", "**Data Subject**" (which includes "**Consumer**"), "**Processing**", "**Personal Data**" (which includes "**Personal Information**"), and "**Sell**" (which includes "**Share**" under the CCPA) (and similar or related variations of such terms) shall have the meanings ascribed to them in the applicable Data Protection Laws.

B. "**Customer Personal Data**" means any Personal Data that is transmitted, stored, or otherwise Processed by or through your Customer Applications in connection with Kinsta's provision of the Services.
C. "**Personal Data Breach**" means any accidental or unauthorized destruction, loss, alteration, disclosure of, or access to, any Customer Personal Data, but excluding unsuccessful attempts or activities that do not compromise the security or integrity of Customer Personal Data, including, but not limited to, log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
D. "**EU Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"), as implemented and supplemented by the domestic legislation of each Member State, the UK Data Protection Act 2018 and the UK GDPR, and the Swiss Data Protection Act, and in each case, as amended, replaced, or superseded from time to time.
E. "**US Data Protection Laws**" means the California Consumer Privacy Act (as amended by the California Privacy Rights Act) (collectively, the "**CCPA**"), the Colorado Privacy Act, the Connecticut Personal Data Privacy and Online Monitoring Act, the Indiana Consumer Data Protection Act, the Iowa Consumer Data Protection Act, the Montana Consumer Data Privacy Act, the Tennessee Information Protection Act, the Virginia Consumer Data Protection Act, the Utah Consumer Privacy Act, and in each case, as amended, replaced, or superseded from time to time.
F. "**Data Protection Laws**" means the laws and regulations relating to the privacy, integrity, and security of Customer Personal Data, including the EU Data Protection Laws and the US Data Protection Laws, which apply to Kinsta's Processing of your Customer Personal Data.
G. "**International Transfer**" means an export of
    a. Customer Personal Data,
    b. governed by any of the EU Data Protection Laws,
    c. to a third country outside the European Economic Area ("EEA"), United Kingdom ("UK"), or Switzerland,
    d. which is not designated by the European Commission, UK, or Switzerland as ensuring an adequate level of protection.
H. "**SCCs**" means the standard contractual clauses, as adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses

for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

I. "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner's Office, VERSION B1.0, in force 21 March 2022.

3. Roles, General Obligations, and CCPA Provisions

A. Customer is the Controller and Business and Kinsta is the Processor and Service Provider with respect to Customer Personal Data. Kinsta shall only Process Customer Personal Data for the purpose of providing the Services in accordance with Customer'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 your instructions violate the Data Protection Laws. The nature, purpose, and duration of the Processing are set forth in SCCs Annex I.

B. Kinsta certifies, understands, and agrees it shall not
    a. Sell Customer Personal Data,
    b. retain, use, or disclose Customer Personal Data for any purpose (including any commercial purpose) other than the specific purpose of performing the Services pursuant to the Agreement, unless expressly permitted by the CCPA, or
    c. retain, use, or disclose Customer Personal Data outside the direct business relationship between you and Kinsta, unless expressly permitted by the CCPA.

    We will inform you if we determine we can no longer meet our obligations under the CCPA.

C. Customer and Kinsta shall comply with the Data Protection Laws. Customer shall obtain any required authorizations, consents, releases, or permissions, and provide all required privacy notices, regarding the Customer Personal Data. For the avoidance of doubt, except as otherwise provided in this DPA, Customer shall have sole responsibility for the accuracy, quality, and legality of all Customer Personal Data and the bases on which it is collected from the Data Subject.

4. Security and Impact Assessments

A. Kinsta shall ensure that its personnel are subject to binding obligations of confidentiality with respect to Customer Personal Data.
B. 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 organizational measures to ensure a level of security appropriate to the risk, including the measures set forth in SCCs Annex II.
C. Taking into account the nature of Processing and the information available to Kinsta, Kinsta shall assist the Customer in ensuring compliance with Customer's obligations under the Data Protection Laws with respect to security, impact assessments, and consultations with supervisory authorities or regulators.

5. Personal Data Breach

A. Taking into account the nature of Processing and the information available to Kinsta, Kinsta shall assist the Customer in ensuring compliance with Customer's obligations under the Data Protection Laws with respect to a Personal Data Breach.
B. If we discover a Personal Data Breach, Kinsta shall, without undue delay, provide written notice to Customer's technical and account contacts, including the Company Owner, using those means established for routine account-related communications.
C. Our notice shall include the following to the extent then known (and updated 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 Customer Personal Data involved in the Personal Data Breach, either specifically, or by reference to the data categories, and
    d. the measures planned or underway to remedy or mitigate the vulnerability giving rise to the Personal Data Breach.

6. Data Subject Requests

A. Taking into account the nature of the Processing, Kinsta shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Laws.
B. Kinsta will promptly notify Customer if we receive a request from a Data Subject to invoke their rights with respect to Customer Personal Data, unless otherwise prohibited by applicable law. We will not independently take any action in response to a request from a Data Subject without Customer's prior written instruction, except as required by applicable law.

7. Data Centers and International Transfers

A. You choose the Google Cloud Platform data center(s) where your Customer Applications will be hosted. You acknowledge, agree, and understand that:
    a. All of your Customer Personal Data will be automatically transferred and stored in the Google data center you choose.
    b. Depending on your choice, Customer Personal Data may be transferred from the EEA, UK, or Switzerland to the country where the Google data center is located.
B. Kinsta and Google have agreed to the Cloud Data Processing Addendum (including the SCCs). For additional information, see Google's commitments regarding cross-border transfers in the "International Data Transfer" section here: https://cloud.google.com/security/gdpr/.
C. Notwithstanding Customer's data center selection, certain aspects of the Services may require International Transfers. Customer authorizes such International Transfers of Customer Personal Data for the sole purpose of providing the Services. International Transfers are subject to MODULE TWO (controller to processor) of the SCCs. For International Transfers from Switzerland, the parties agree that all adaptations and amendments to the SCCs required by the Swiss Federal Data Protection and Information Commissioner are incorporated into the SCCs (the "**Swiss Amendments**"). For International Transfers from the United Kingdom, the parties agree to the UK

Addendum. The UK Addendum Table information is as follows: Table 1: See SCC Annex I below; Table 2: See Section 7.D below; Table 3: See SCCs Annex I and II below; the list of Kinsta's Sub-processors is located here: https://kinsta.com/legal/subprocessors/; Table 4: Importer and exporter may end the UK Addendum as set out in Section 19 thereof.

D. Regarding optional provisions in the SCCs, Swiss Amendments, and UK Addendum, the parties agree as follows:
    a. The parties agree to Clause 7.
    b. The parties choose OPTION 2 in Clause 9(a).
    c. The parties do not agree to the optional provisions of Clause 11(a).
    d. The parties choose OPTION 1 in Clause 17 and the Member State shall be Ireland, the UK, or Switzerland, as applicable.
    e. The parties agree that the Member State in Clause 18(b) shall be Ireland, the UK, or Switzerland, as applicable.
E. The SCCs, Swiss Amendments, and UK Addendum, as applicable, are incorporated by reference into this DPA for any International Transfers. The parties' acceptance of the Agreement shall serve as their respective agreement to comply with the relevant SCCs, Swiss Amendments, and UK Addendum with respect to any International Transfers.

8. Sub-processors

A. Kinsta engages third-party subcontractors that Process Customer Personal Data ("**Sub-processors**") for the purpose of providing the Services. A current list of Sub-processors is available here: https://kinsta.com/legal/subprocessors/ (the "**Sub-processor List**"). Customer authorizes Kinsta to engage these Sub-processors for the purpose of providing the Services.
B. Prior to adding or replacing any Sub-processors, Kinsta will provide written notice of such changes to the Company Owner contact listed in MyKinsta. Customer's failure to object in writing to a new Sub-processor within 14 days of Kinsta's notification of the new Sub-processor shall constitute Customer's authorization of the new Sub-processor.
C. If Kinsta determines in its sole discretion that it cannot reasonably accommodate Customer's timely objection to a Sub-processor, upon notice from Kinsta, Customer may

choose to terminate the Agreement pursuant to the termination provisions in the Terms of Service, which shall be Customer's sole and exclusive remedy.

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

9. Audit and Inspection

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

B. Any audits requested by Customer to assess and verify compliance with this DPA 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 confidentiality and non-disclosure agreement and a detailed written audit plan reviewed and pre-approved by Kinsta; (iii) limited to once every twelve (12) month period; (iv) at Customer'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 Customer has exhausted all other reasonable means as determined by Kinsta; and (vi) in the virtual or physical presence of a Kinsta representative without unreasonably disrupting Kinsta's business operations.

10. Deletion or Return of Customer Personal Data

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

SCCs Annex I

A. **LIST OF PARTIES**

Data Exporter:

Name: The entity identified as the Customer.

Address: The address for Customer recorded in MyKinsta or as otherwise specified in the Agreement.

Contact name, position, and contact details: The contact details of the Company Owner associated with Customer's Account, or as otherwise specified in the Agreement.

Activities related to the data transferred under the Clauses: Operation of Customer Applications(s) on Kinsta's hosting platform

Signature and date: The parties agree that acceptance or executions of the Agreement, as applicable, shall constitute execution of these SCCs by both parties.

Role: Controller

Data Importer:

Name: Kinsta Inc.

Address: 8605 Santa Monica Blvd #92581, West Hollywood, CA 90069, USA

Contact name, position, and contact details: Kinsta Data Privacy team privacy@kinsta.com or by mail at address above

Activities related to the data transferred under the Clauses: Provision of the Services

Signature and date: The parties agree that acceptance or executions of the Agreement, as applicable, shall constitute execution of these SCCs by both parties.

Role: Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Any individuals who may visit, use, or access Customer Applications, or whose personal data is transmitted, stored, or otherwise processed through Customer Applications by the Customer, including, for example: employees and other staff, customers and clients (including their staff), website visitors or end users, suppliers (including their staff), relatives and associates of the above, advisers, consultants and other professional experts, shareholders, members or supporters, and students and pupils.

Categories of personal data transferred

Any categories permitted by Customer to be transmitted, stored, or otherwise processed through the Customer Applications. Such categories may include, for example, contact information, employment details, financial information, education and training details, identifiers by a public authority, family, lifestyle and social circumstances.

Sensitive data transferred (if applicable) and applied restrictions

Customer may permit sensitive data to be transmitted, stored, or otherwise processed through the Customer Applications. The restrictions and safeguards specified in Annex II apply to these categories of personal data (if any). Customer shall be responsible for informing Kinsta of the specific categories of sensitive data transferred and any additional applied restrictions.

The frequency of the transfer

Continuous

Nature of the processing

Processing in connection with the provision of the Services, including hosting of the Customer Applications and related support.

Purpose(s) of the data transfer and further processing

Provision of the Services

The period for which the personal data will be retained

Pursuant to DPA, Section 10

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

The subject matter, nature, and duration of the processing by sub-processors are set forth in this Annex I, Section B.

C. **COMPETENT SUPERVISORY AUTHORITY**

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

Ireland

SCCs Annex II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA.

- All Customer Personal Data transferred by Kinsta is encrypted in transit.
- All Customer Personal Data stored on Google Cloud infrastructure (all Customer Applications and access logs) is encrypted at rest.
- Cloudflare's security features, including their web application firewall (WAF) and DDoS protection, are integrated into the Services.
- We have information security policies which restrict our team members' activities related to the processing of Customer Personal Data to only those processing activities which are necessary for the provision of the Services.
- All team members sign an agreement inclusive of non-disclosure provisions prior to gaining access to any Customer Personal Data.
- We have a dedicated full time Security team.
- We have identified a Security oversight group that includes members of our Engineering, Operations, Legal, and Executive teams.
- Sub-processors of Customer Personal Data are only used after formal review and approval.
- We make reasonable efforts to process, transfer, and retain only the amount and type of data required to provide the Services.

- We have established identity and access management policies and practices, following the principles of least privilege and role-based access control (RBAC).
- All team members receive training on matters of data privacy and our policies.
- Physical access controls have been implemented by Google Cloud to limit access to physical hardware at data centers. Google Cloud has also received multiple security-related certifications and audits including a SOC 2 Type II report and ISO 27001 certification.
- Where applicable, two-factor authentication has been enabled on all team member accounts with access to Customer Personal Data.
- Root access to client containers and servers is by unique private key only, and team members are only provided the minimum access necessary to perform their duties.
- Root access is only possible via dedicated network access points and not the same access points as regular client access.
- Kinsta offers free SSL certificates and makes it possible for Customers to force HTTPS connections to encrypt all Customer Application traffic in transit.
- Kinsta limits non-HTTP connections to secure protocols only (SSH, SFTP).
- Customer Applications are protected by a custom firewall managed by Kinsta's Engineering team.
- Multiple forms of regular backups are created. Customers are able to easily download backups for transfer to other hosts (portability) or for storage on other services.
- Customers are able to initiate deletion of Customer Applications from the platform. Upon termination of the Services, Kinsta makes reasonable efforts to delete all Customer Personal Data within 45 days.
- Server packages and software are kept up to date by our Engineering team. Security updates are applied promptly.