Vercel

DATA PROTECTION ADDENDUM

1. Introduction

This Data Protection Addendum ("**Addendum**") is entered into as of the date last signed by Customer below ("Effective Date") and is by and between Vercel Inc., a Delaware corporation ("**Vercel**"), and Customer. This Addendum applies to Vercel's Processing of Personal Data under the Vercel Enterprise Services Order Form and Enterprise Terms and Conditions or other agreement executed between Vercel and Customer for Vercel's provision of Services (the "**Agreement**").

Customer enters into this Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Affiliates to the extent such Affiliates are included and covered under the Agreement with Vercel. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Affiliates.

This Addendum has been pre-signed on behalf of Vercel. To complete this Addendum, Customer must complete the information in the signature box and send the executed Addendum to Vercel by email to privacy@vercel.com indicating, if applicable, Customer's account number. Except as otherwise expressly provided in the Agreement, this Addendum shall become legally binding upon receipt by Vercel of the validly completed Addendum at the above email address.

2. Definitions

Capitalized terms that are used but not defined in this Addendum have the meanings given in the Agreement.

a. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interest of the subject entity.

b. "**Applicable Data Protection Laws**" means, with respect to a party, all privacy, data protection and information security-related laws and regulations applicable to such party's Processing of Personal Data.

c. "**Customer Data**" means Your Data (as defined in the Agreement) that constitutes Personal Data.

d. "**Data Subject**" means the identified or identifiable natural person who is the subject of Personal Data.

e. "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

f. "**Personal Data**" means "personal data", "personal information", "personally identifiable information" or similar information defined in and governed by Applicable Data Protection Laws.

g. "**Security Incident**" means any confirmed unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data being Processed by Vercel. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

h. "**Subprocessor**" means any third party authorized by Vercel to Process any Customer Data.

i. "**Usage Data**" means aggregate and other usage data that is not Your Data. This Addendum applies to Usage Data to the extent Usage Data constitutes Personal Data.

3. General; Termination

a. This Addendum forms part of the Agreement and except as expressly set forth in this Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Agreement, this Addendum will govern.

b. Any liabilities arising under this Addendum are subject to the limitations of liability in the Agreement.

c. This Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

d. This Addendum will automatically terminate upon expiration or termination of the Agreement.

4. Relationship of the Parties

a. Vercel as Processor. The parties acknowledge and agree that with regard to the Processing of Customer Data, Customer acts as a controller and Vercel is a processor. Vercel will process Customer Data in accordance with Customer's instructions as outlined in Section 6 (Role and Scope of Processing).

b. Vercel as Controller. To the extent that any Usage Data (as defined in the Agreement) is considered Personal Data, Vercel is the controller with respect to such data and will Process such data in accordance with its Privacy Policy.

5. Compliance with Law. Each party will comply with its obligations under Applicable Data Protection Laws with respect to its Processing of Customer Data.

6. Role and Scope of the Processing

a. Customer Instructions. Vercel will Process Customer Data only in accordance with Customer's instructions. By entering into the Agreement, Customer instructs Vercel to Process Customer Data to provide the Services and pursuant to any other written instructions given by Customer and acknowledged in writing by Vercel as constituting instructions for purposes of this Addendum. Customer acknowledges and agrees that such instruction authorizes Vercel to Process Customer Data (a) to perform its obligations and exercise its rights under the Agreement; and (b) to perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement.

7. <u>Subprocessing</u>

a. Customer specifically authorizes Vercel to use its Affiliates as Subprocessors, and generally authorizes Vercel to engage Subprocessors to Process Customer Data. In such instances, Vercel:

(i) will enter into a written agreement with each Subprocessor, imposing data protection obligations substantially similar to those set out in this Addendum; and

(ii) remains liable for compliance with the obligations of this Addendum and for any acts or omissions of the Subprocessor that cause Vercel to breach any of its obligations under this Addendum.

b. A list of Vercel's Subprocessors, including their functions and locations, is available at https://vercel.com/legal/sub-processors, and may be updated by Vercel from time to time in accordance with this Addendum.

c. When any new Subprocessor is engaged, Vercel will notify Customer of the engagement, which notice may be given by updating the Subprocessor Page and/or via a message through email or the Service. Vercel will give such notice at least ten (10) calendar days before the new Subprocessor Processes any Customer Data, except that if Vercel reasonably believes engaging a new Subprocessor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Customer Data or avoid material disruption to the Services, Vercel will give such notice as soon as reasonably practicable. If, within five (5) calendar days after such notice, Customer notifies Vercel in writing that Customer objects to Vercel's appointment of a new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith and whether they can be resolved. If the parties are not able to mutually agree to a resolution of such concerns, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience with no refunds and Customer will remain liable to pay any committed fees in an order form, order, statement of work or other similar ordering document.

8. <u>Security</u>

a. <u>Security Measures.</u> Vercel will implement and maintain technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with Vercel's security standards referenced in the Agreement ("**Security Measures**").

b. <u>Customer Responsibility.</u>

(i) Customer is responsible for reviewing the information made available by Vercel relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Applicable Data Protection Laws. Customer acknowledges that the Security Measures may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices (but the modifications will not materially decrease Vercel's obligations as compared to those reflected in such terms as of the Effective Date).

(ii) Customer agrees that, without limitation of Vercel's obligations under this Section 8, Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that it uses with the Services; and (d) maintaining its own backups of Customer Data.

c. Security Incident. Upon becoming aware of a confirmed Security Incident, Vercel will notify Customer without undue delay unless prohibited by applicable law. A delay in giving such notice requested by law enforcement and/or in light of Vercel's legitimate needs to investigate or remediate the matter before providing notice will not constitute an undue delay. Such notices will describe, to the extent possible, details of the Security Incident, including steps taken to mitigate the potential risks and steps Vercel recommends Customer take to address the Security Incident. Without prejudice to Vercel's obligations under this Section 8.c., Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Security Incidents. Vercel's notification of or response to a Security Incident under this Section 8.c. will not be construed as an acknowledgement by Vercel of any fault or liability with respect to the Security Incident.

9. Audits and Reviews of Compliance. The parties acknowledge that Customer must be able to assess Vercel's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as Vercel is acting as a processor on behalf of Customer.

a. Vercel's Audit Program. Vercel uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Data and is SOC2 Type 2 compliant. Such audits are performed at least once annually at Vercel's expense by independent third-party security professionals at Vercel's selection and result in the generation of a confidential audit report ("**Audit Report**"). For more information on Vercel's security measures please see our Security FAQs at https://vercel.com/security#faqs.

b. Customer Audit. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Vercel will make available to Customer a copy of Vercel's most recent Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Laws will be satisfied by these Audit Reports. To the extent that Vercel's provision of an Audit Report does not provide sufficient information for Customer to verify Vercel's compliance with this Addendum or Customer is required to respond to a regulatory authority audit, Customer agrees to a mutually agreed-upon audit plan with Vercel that: (a) ensures the use of an independent third party; (b) provides notice to Vercel in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Customer at Vercel's then-current rates; (e) occurs no more than once annually; (f) restricts findings to only Customer Data relevant to Customer; and (g) obligates Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

10. Impact Assessments and Consultations. Vercel will provide reasonable cooperation to Customer in connection with any data protection impact assessment (at Customer's expense only if such reasonable cooperation will require Vercel to assign significant resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Laws.

11. Data Subject Requests. Vercel will upon Customer's request (and at Customer's expense) provide Customer with such assistance as it may reasonably require to comply with its obligations under Applicable Data Protection Laws to respond to requests from individuals to exercise their rights under Applicable Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection) in cases where Customer cannot reasonably fulfill such requests independently by using the self-service functionality of the Services. If Vercel receives a request from a Data Subject in relation to their Customer Data, Vercel will advise the Data Subject to submit their request to Customer, and Customer will be responsible for responding to any such request.

12. Return or Deletion of Customer Data

a. Vercel will, within sixty (60) days after request by Customer following the termination or expiration of the Agreement, delete all Customer Data from Vercel’s systems.

b. Notwithstanding the foregoing, Customer understands that Vercel may retain Customer Data if required by law, and such data will remain subject to the requirements of this Addendum.

13. International Provisions

a. Processing in the United States. Customer acknowledges that, as of the Effective Date, Vercel’s primary processing facilities are in the United States.

b. Jurisdiction Specific Terms. To the extent that Vercel Processes Customer Data originating from and protected by Applicable Data Protection Laws in one of the Jurisdictions listed in Schedule 4 (Jurisdiction Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this Addendum.

c. Cross Border Data Transfer Mechanism. To the extent that Customer’s use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area (“**EEA**”), the United Kingdom (“**UK**”), Switzerland or any other jurisdiction listed in Schedule 3) to Vercel located outside of that jurisdiction (a “**Transfer Mechanism**”), the terms and conditions of Schedule 3 (Cross Border Transfer Mechanisms) will apply.

“Vercel”

VERCEL INC.

By: Kevin Van Gundy

Name: Kevin Van Gundy

Title: Chief Revenue Officer

Date: 2021-10-05

“Customer”

____

By:

Name:

Title:

Date:

SCHEDULE 1

SUBJECT MATTER & DETAILS OF PROCESSING

1. Nature and Purpose of the Processing. Vercel will process Personal Data as necessary to provide the Services under the Agreement. Vercel does not sell Customer Data (or end user information within such Customer Data) and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

a. Customer Data. Vercel will process Customer Data as a processor in accordance with Customer's instructions as outlined in Section 6.a (Customer Instructions) of this Addendum.

b. Usage Data. Vercel will process Usage Data as a controller for the purposes outlined in Section 4.b (Vercel as Controller) of this Addendum.

2. Processing Activities.

a. Customer Data. Customer Data will be subject to the following basic processing activities: the provision of Services.

b. Usage Data. Personal Data contained in Usage Data will be subject to the following processing activities by Vercel: Vercel may use Usage Data to operate, improve and support the Services and for other lawful business practices, such as analytics, benchmarking and reporting.

3. Duration of the Processing. The period for which Personal Data will be retained and the criteria used to determine that period is as follows:

a. Customer Data. Prior to the termination of the Agreement, Vercel will process stored Customer Data for the purpose of providing the Services until Customer elects to delete such Customer Data via the Vercel Services or in accordance with the Agreement.

b. Usage Data. Upon termination of the Agreement, Vercel may retain, use and disclose Usage Data for the purposes set forth above in Section 2.b (Usage Data) of this Schedule 1, subject to the confidentiality obligations set forth in the Agreement. Vercel will anonymize or delete Personal Data contained within Usage Data when Vercel no longer requires it for the purpose set forth in Section 2.b (Usage Data) of this Schedule 1.

4. Categories of Data Subjects.

a. Customer Data. Customer's customers, employees, suppliers and end-users.

b. Usage Data: Customer's authorized users with access to a Vercel account, customers, suppliers and end-users.

5. Categories of Personal Data.

a. Customer Data. The categories of Customer Data are such categories as Customer is authorized to ingest into the Services under the Agreement.

b. Usage Data. Vercel processes Personal Data within Usage Data.

6. Sensitive Data or Special Categories of Data.

a. Customer Data. Customers are prohibited from including sensitive data or special categories of data in Customer Data.

b. Usage Data. Sensitive Data is not contained in Usage Data.

SCHEDULE 2

TECHNICAL & ORGANIZATIONAL SECURITY MEASURES

Where applicable, this Schedule 2 will serve as Annex II to the Standard Contractual Clauses. The following provides more information regarding Vercel's technical and organizational security measures set forth below.

Technical and Organizational Security Measures:

1. Measures of pseudonymization and encryption of personal data.

Vercel maintains Customer Data in an encrypted format at rest using Advanced Encryption Standard and in transit using TLS.

2. Measures for ensuring ongoing confidentiality, integrity, and availability and resilience of processing systems and services.

Vercel's customer agreements contain strict confidentiality obligations. Additionally, Vercel requires every downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in Vercel's customer agreements. The infrastructure for the Vercel Services spans multiple fault-independent AWS availability zones in geographic regions physically separated from one another, supported by various tools and processes to maintain high availability of services.

3. Measures for ensuring the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

Vercel performs regular backups of Customer Data, which is hosted in AWS, Microsoft Azure, and GCS data centers. Backups are retained redundantly across multiple availability zones and encrypted in-transit and at-rest using Advanced Encryption Standard (AES-256).

4. Processes for regular testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of processing.

Vercel maintains a risk-based assessment security program. The framework for Vercel's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. Vercel's security program is intended to be appropriate to the nature of the Services and the size and complexity of Vercel's business operations. Vercel has a separate and dedicated security team that manages Vercel's security program. This team facilitates and supports independent audits and assessments performed by third-parties to provide independent feedback on the operating effectiveness of the information security program.

5. Measures for user identification and authorization.

Vercel personnel are required to use unique user access credentials and passwords for authorization. Vercel follows the principles of least privilege through role-based and time-based access models when provisioning system access. Vercel personnel are authorized to access Customer Data based on their job function, role and responsibilities, and such access requires approval prior to access provisioning. Access is promptly removed upon role change or termination.

6. Measures for the protection of data during transmission.

   Customer Data is encrypted when in-transit between Customer and Vercel Service using TLS.

7. Measures for the protection of data during storage.

   Customer Data is stored encrypted using the Advanced Encryption Standard.

8. Measures for ensuring physical security of locations at which personal data are processed.

   Vercel headquarters and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security. All employees, contractors, and visitors are required to identify themselves and have unique access tokens. Physical security controls are inherited from our co-working office provider.

   The Services operate on Amazon Web Services (“**AWS**”), Microsoft Azure (**"Azure"**), and Google Cloud (“**GCS**”) and are protected by the security and environmental controls of Amazon and Google, respectively.

   Detailed information about AWS security is available at:
   - https://aws.amazon.com/security/ and
   - http://aws.amazon.com/security/sharing-the-security-responsibility/.
   For AWS SOC Reports, please see:
   - https://aws.amazon.com/compliance/soc-faqs/
   Detailed information about Azure security is available at:
   - https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security.
   Detailed information about GCS security is available at
   - https://cloud.google.com/docs/tutorials#security.

9. Measures for ensuring events logging.

   Vercel monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is centralized by the security team. Log activities are investigated when necessary and escalated appropriately.

10. Measures for ensuring systems configuration, including default configuration.

    Vercel applies Secure Software Development Lifecycle (Secure SDLC) standards to perform numerous security-related activities for the Services across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before new Services are deployed; (b) bi-annual penetration testing by independent third parties; and (c) threat models for new Services to detect any potential security threats and vulnerabilities.

    Vercel adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. Monitors are in place to notify the security team of changes made to critical infrastructure and services that do not adhere to the change management processes.

11. Measures for internal IT and IT security governance and management.

Vercel maintains a risk-based assessment security program. The framework for Vercel's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. Vercel's security program is intended to be appropriate to the nature of the Services and the size and complexity of Vercel's business operations. Vercel has a separate and dedicated Information Security team that manages Vercel's security program. This team facilitates and supports independent audits and assessments performed by third parties. Vercel's security framework is based on the ISO 27001 Information Security Management System and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response. Security is managed at the highest levels of the company, with security and technology leadership meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all Vercel employees for their reference.

12. Measures for certifications/assurance of processes and products.

    Vercel conducts various third-party audits to attest to various frameworks including ISO 27001, SOC 2 Type 2, and bi-annual application penetration testing.

13. Measures for ensuring data minimization.

    Vercel Customers unilaterally determine what Customer Data they route through the Vercel Services and how the Services are configured. As such, Vercel operates on a shared responsibility model. Vercel provides tools within the Services that gives Customers control over exactly what data enters the platform and enables Customers with the ability to block data at the Source level. Additionally, Vercel allows Customers to delete and suppress Customer Data on demand.

14. Measures for ensuring data quality.

    Vercel has a three-fold approach for ensuring data quality. These measures include: (i) unit testing to ensure the quality of logic used to make API calls, (ii) volume testing to ensure the code is able to scale, and (iii) daily end-to-end testing to ensure that the input values match expected values. Vercel applies these measures across the board, both to ensure the quality of any Usage Data that Vercel collects and to ensure that the Vercel Platform is operating in accordance with the documentation.

    Each Vercel Customer chooses what Customer Data they route through the Vercel Services and how the Services are configured. As such, Vercel operates on a shared responsibility model. Vercel ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data leaves Vercel to flow to a downstream destination.

15. Measures for ensuring limited data retention.

    Vercel Customers unilaterally determine what Customer Data they route through the Vercel Services and how the Services are configured. As such, Vercel operates on a shared responsibility model. If a Customer is unable to delete Customer Data via the self-services functionality of the Services, then Vercel deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law.

16. Measures for ensuring accountability.

Vercel has adopted measures for ensuring accountability, such as implementing data protection policies across the business, publishing Vercel's Information Security Policy (available at https://vercel.com/security), maintaining documentation of processing activities, and recording and reporting Security Incidents involving Personal Data. Vercel conducts regular third-party audits to ensure compliance with our privacy and security standards.

17. Measures for allowing data portability and ensuring erasure.

Vercel's Customers have direct relationships with their end users and are responsible for responding to requests from their end users who wish to exercise their rights under Applicable Data Protection Laws. Vercel has functionality that allows Customers to delete and suppress Customer Data. Vercel specifies in the Data Protection Addendum that it will provide assistance to such Customer as may reasonably be require to comply with Customer's obligations under Applicable Data Protection Laws to respond to requests from individuals to exercise their rights under Applicable Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection). If Vercel receives a request from a Data Subject in relation to their Customer Data, Vercel will advise the Data Subject to submit their request to Customer, and Customer will be responsible for responding to any such request.

18. For transfers to [sub]-processors, also describe the specific technical and organisational measures to be taken by the [sub]-processor to be able to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the data exporter.

When Vercel engages a sub-processor under this Addendum, Vercel and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that Vercel is able to meet its obligations to Customer. In addition to implementing technical and organisational measures to protect personal data, sub-processors must a) notify Vercel in the event of a Security Incident so Vercel may notify Customer; b) delete data when instructed by Vercel in accordance with Customer's instructions to Vercel; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or e) process data in a manner which conflicts with Customer's instructions to Vercel.

SCHEDULE 3

CROSS BORDER DATA TRANSFER MECHANISM

1. **Definitions**

a. **"Standard Contractual Clauses"** means, depending on the circumstances unique to any particular Customer, any of the following:

(i) UK Standard Contractual Clauses; and

(ii) 2021 Standard Contractual Clauses

b. "**UK Standard Contractual Clauses**" means:

(i) Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU ("**UK Controller to Processor SCCs**"); and

(ii) Standard Contractual Clauses for data controller to data controller transfers approved by the European Commission in decision 2004/915/EC (“**UK Controller to Controller SCCs”**).

c. "**2021 Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

2. UK Standard Contractual Clauses. For data transfers from the United Kingdom that are subject to the UK Standard Contractual Clauses, the UK Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by reference) and completed as follows:

a. The UK Controller to Processor SCCs will apply where Vercel is processing Customer Data. The illustrative indemnification clause will not apply. Schedule 1 serves as Appendix 1 of the UK Controller to Processor SCCs. Schedule 2 serves as Appendix 2 of the UK Controller to Processor SCCs.

b. The UK Controller to Controller SCCs will apply where Vercel is processing Usage Data. In Clause II(h), Vercel will process personal data in accordance with the data processing principles set forth in Annex A of the UK Controller to Controller SCCs. The illustrative commercial clause will not apply. Schedule 1 serves as Annex B of the UK Controller to Controller SCCs. Personal Data transferred under these clauses may only be disclosed to the following categories of recipients: i) Vercel’s employees, agents, Affiliates, advisors and independent contractors with a reasonable business purpose for needing such personal data; ii) Vercel vendors that, in their performance of their obligations to Vercel, must process such personal data acting on behalf of and according to instructions from Vercel; and iii) any person (natural or legal) or organisation to whom Vercel may be required by applicable law or regulation to disclose personal data, including law enforcement authorities, central and local government.

3. The 2021 Standard Contractual Clauses. For data transfers from the European Economic Area, the UK, and Switzerland that are subject to the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will apply in the following manner:

a. Module One (Controller to Controller) will apply where Customer is a controller of Usage Data and Vercel is a controller of Usage Data.

b. Module Two (Controller to Processor) will apply where Customer is a controller of Customer Data and Vercel is a processor of Customer Data;

d. For each Module, where applicable:

(i) in Clause 7, the option docking clause will not apply;

(ii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes will be as set forth in Section 7 (Subprocessing) of this Addendum;

(iii) in Clause 11, the optional language will not apply;

(iv) in Clause 17 (Option 1), the 2021 Standard Contractual Clauses will be governed by Irish law.

(v) in Clause 18(b), disputes will be resolved before the courts of Ireland;

(vi) In Annex I, Part A:

Data Exporter: Customer and authorized Affiliates of Customer.

Contact Details: Customer's account owner email address, or to the email address(es) for which Customer elects to receive privacy communications.

Data Exporter Role: The Data Exporter's role is outlined in Section 4 of this Addendum.

Signature & Date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data Importer: Vercel Inc.

Contact Details: Vercel Privacy Team – privacy@vercel.com

Data Importer Role: The Data Importer's role is outlined in Section 4 of this Addendum.

Signature & Date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

(vii) In Annex I, Part B:

The categories of data subjects are described in Schedule 1, Section 4.

The sensitive data transferred is described in Schedule 1, Section 6.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is described in Schedule 1, Section 1.

The purpose of the processing is described in Schedule 1, Section 1.

The period of the processing is described in Schedule 1, Section 3.

For transfers to sub-processors, the subject matter, nature, and duration of the processing is outlined at https://vercel.com/legal/sub-processors.

(viii) In Annex I, Part C: The Irish Data Protection Commission will be the competent supervisory authority.

(ix) Schedule 2 serves as Annex II of the Standard Contractual Clauses.

4. As to the specific modules, the parties agree that the following modules apply, as the circumstances of the transfer may apply:

Controller-Controller - Module One

Controller-Processor - Module Two

5. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this Addendum, including Schedule 4 (Jurisdiction Specific Terms), the provisions of the Standard Contractual Clauses will prevail.

SCHEDULE 4

JURISDICTION SPECIFIC TERMS

1. California

a. The definition of "**Applicable Data Protection Law**" includes the California Consumer Privacy Act ("**CCPA**").

b. The terms "**business**", "**commercial purpose**", "**service provider**", "**sell**" and "**personal information**" have the meanings given in the CCPA.

c. With respect to Customer Data, Vercel is a service provider under the CCPA.

d. Vercel will not (a) sell Customer Data; (b) retain, use or disclose any Customer Data for any purpose other than for the specific purpose of providing the Services, including retaining, using or disclosing the Customer Data for a commercial purpose other than providing the Services; or (c) retain, use or disclose the Customer Data outside of the direct business relationship between Vercel and Customer.

e. The parties acknowledge and agree that the Processing of Customer Data authorized by Customer's instructions described in Section 6 of this Addendum is integral to and encompassed by Vercel's provision of the Services and the direct business relationship between the parties.

f. Notwithstanding anything in the Agreement or any Order Form entered in connection therewith, the parties acknowledge and agree that Vercel's access to Customer Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

g. To the extent that any Usage Data (as defined in the Agreement) is considered Personal Data, if and when Vercel is subject to the CCPA, Vercel is the business under the CCPA with respect to such data and will Process such data in accordance with its Privacy Policy. As of October 1, 2021 Vercel is not subject to the CCPA as a business.

2. EEA

a. The definition of "**Applicable Data Protection Laws**" includes the General Data Protection Regulation (EU 2016/679)("**GDPR**").

b. When Vercel engages a Subprocessor under Section 7 (Subprocessing), it will:

(i) require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(ii) require any appointed Subprocessor to agree in writing to only process data in a country that the European Union has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses.

c. GDPR Penalties. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

3. Switzerland

a. The definition of “Applicable Data Protection Laws” includes the Swiss Federal Act on Data Protection.

b. When Vercel engages a Subprocessor under Section 7 (Subprocessing), it will

(i) require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(ii) require any appointed Subprocessor to agree in writing to only process data in a country that the European Union has declared to have an “adequate” level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses.

4. United Kingdom

a. References in this Addendum to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

b. When Vercel engages a Subprocessor under Section 7 (Subprocessing), it will:

(i) require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(ii) require any appointed Subprocessor to agree in writing to only process data in a country that the European Union has declared to have an “adequate” level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses.