DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is an agreement between Vercel, Inc. ("Vercel," “we,” “us,” or “our”) and you or the entity you represent ("Customer", “you” or “your”). This DPA supplements the Vercel Enterprise Services Order Form and Enterprise Terms and Conditions, as updated from time to time between Customer and Vercel, or any other agreement between Customer and Vercel governing Customer’s use of the Services (collectively, “Services Agreement”). This DPA applies when any Customer Data processed by Vercel is subject to the GDPR (as defined below).

1. **Definitions.** Unless otherwise defined in the Services Agreement, all capitalized terms used in this DPA will have the meanings given to them below or as set forth in the GDPR:

1.1. "Vercel Network" means Vercel’s owned or utilized facilities, servers, networking equipment, and host software systems (e.g., virtual private clouds) that are within Vercel’s control and are used to provide the Services.

1.2. "Vercel Security Standards" means the security standards attached to the Services Agreement, or if none are attached to the Services Agreement, attached to this DPA as Annex 1.

1.3. "Customer" means you or the entity you represent.

1.4. "Customer Data" means the “Personal Data” (as defined under GDPR) that is uploaded by Customer to the Services under Customer’s Vercel accounts.

1.5. "EEA" means the European Economic Area.

1.6. "Data Protection Legislation" means (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the European Directives 95/46 and 2002/58/EC (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them; (ii) all relevant Member State laws or regulations giving effect or corresponding with the GDPR; (iii) any implementing legislation or legislation having equivalent effect in the United Kingdom to the extent the United Kingdom is no longer a Member State; and (iv) any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant supervisory authority and binding under applicable law.

1.7. "Processing" has the meaning given to it under GDPR and “Process”, “Processes” and “Processed” will be interpreted accordingly.

1.8. "Security Incident" means a breach of Vercel’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

2. **Data Processing.** This DPA applies when Customer Data is Processed by Vercel. Vercel will act as a Processor to Customer who may act as “Controller” (as such term is defined by GDPR) or Processor with respect to Customer Data.
2.1. **Customer Controls.** The Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Data as described in the Documentation. Without prejudice to Section 6.1, Customer may use these controls to assist it in connection with its obligations under Data Protection Legislation, including its obligations related to responding to requests from Data Subjects.

2.2. **Details of Data Processing.**
   
a. **Subject matter.** The subject matter of the Processing under this DPA is Customer Data.

b. **Duration.** As between Vercel and Customer, the duration of the Processing under this DPA is determined by Customer.

c. **Purpose.** The purpose of the Processing under this DPA is the provision of the Services initiated by Customer from time to time.

d. **Nature of the Processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

e. **Type of Customer Data.** Customer Data uploaded to the Services under Customer’s Vercel accounts.

f. **Categories of Data Subjects.** Data Subjects may include Customer’s customers, employees, suppliers and end-users.

2.3. **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Data Protection Legislation.

2.4. **Customer Obligations.** Customer is solely responsible for (i) the accuracy, quality, and legality of the Customer Data provided to Vercel by (or on behalf) of Customer, (ii) the means by which Customer acquires any such Customer Data, including establishing all required legal bases (and obtaining and recording consent where consent is required) for the Processing contemplated hereunder, (iii) informing Data Subjects of the Processing of their Personal Data by Vercel (as applicable), and (iv) the instructions it provides to Vercel regarding the Processing of Customer Data. Customer will not provide or make available to Vercel any Customer Data in violation of the Services Agreement, this DPA or Data Protection Legislation, or that is otherwise inappropriate for the nature of the Services to be provided by Vercel, and shall promptly notify Vercel where Customer Data that is Processed by Vercel must no longer be Processed by reason of a Data Subject’s request for deletion or withdrawal of consent, or any other legally valid obligation under Data Protection Legislation that mandates the cessation of Processing by Vercel. If Customer is itself a processor, Customer warrants to Vercel that Customer’s instructions and actions with respect to such Personal Data, including its appointment of Vercel as another Processor, have been authorized by the relevant Controller.

3. **Customer Instructions.** The parties agree that this DPA and the Services Agreement (including the provision of instructions via configuration tools such as the Vercel Command Line Interface and APIs made available by Vercel for the Services) constitute Customer’s documented instructions regarding Vercel’s Processing of Customer Data (“Documented Instructions”). Vercel will Process Customer Data only in accordance with Documented Instructions; provided, however, that such limitations will not apply with respect to Vercel’s (i) internal purposes of
developing anonymized and aggregated usage and performance metrics for reporting or statistical purposes, (ii) security and fraud prevention, and/or (ii) compliance with Vercel’s legal and regulatory obligations. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Vercel and Customer, including agreement on any additional fees payable by Customer to Vercel for carrying out such instructions. Customer is entitled to terminate this DPA and the Services Agreement if Vercel declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

4. **Confidentiality of Customer Data.** Vercel will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a government body (such as a subpoena or court order). If a government body sends Vercel a demand for Customer Data, Vercel will attempt to redirect the government body to request that data directly from Customer. As part of this effort, Vercel may provide Customer’s basic contact information to the government body. If compelled to disclose Customer Data to a government body, Vercel will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Vercel is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Section 4 varies or modifies the Standard Contractual Clauses.

5. **Confidentiality Obligations of Vercel Personnel.** Vercel restricts its personnel from Processing Customer Data without authorization by Vercel as described in the Vercel Security Standards. Vercel imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

6. **Security of Data Processing.**

6.1. Vercel has implemented and will maintain appropriate technical and organizational measures for the Vercel Network as described in this Section. In particular, Vercel has implemented and will maintain the following technical and organizational measures:

   a. security of the Vercel Network as set out in the Vercel Security Standards;

   b. physical security of the facilities as set out in the Vercel Security Standards; measures to control access rights for Vercel employees and contractors in relation to the Vercel Network as set out in the Vercel Security Standards; and

   c. processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Vercel as described in the Vercel Security Standards.

6.2. Customer may elect to implement technical and organizational measures in relation to Customer Data. Such technical and organizational measures include the following which may be obtained by Customer from Vercel, or directly from a third-party supplier:

   a. pseudonymization and encryption to ensure an appropriate level of security;

   b. measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are being operated by Customer;

   c. measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and
d. processes for regularly testing, assessing and evaluating the effectiveness of the
technical and organizational measures implemented by Customer.

7. Sub-processing.

7.1. Authorized Sub-processors. Customer agrees that Vercel may use sub-processors to
fulfill its contractual obligations under this DPA or to provide certain services on its behalf,
such as providing support services. Customer consents to Vercel's use of sub-processors
as described in this Section. Except as set forth in this Section, or as Customer may
otherwise authorize, Vercel will not permit any sub-processor to carry out Processing
activities on Customer Data on behalf of Customer.

7.2. Sub-processor Obligations. Where Vercel authorizes any sub-processor as described in
Section 7.1:

a. Vercel will restrict sub-processor's access to Customer Data to what is necessary to
maintain the Services or to provide the Services to Customer and any End Users in
accordance with the Documentation and Vercel will prohibit the sub-processor from
accessing Customer Data for any other purpose; Vercel will enter into a written
agreement with the sub-processor and, to the extent that the sub-processor is
performing the same Processing services that are being provided by Vercel under
this DPA, Vercel will impose on the sub-processor the same contractual obligations
that Vercel has under this DPA; and

b. Vercel will remain responsible for its compliance with the obligations of this DPA and
for any acts or omissions of the sub-processors that cause Vercel to breach any of
Vercel’s obligations under this DPA.

8. Data Subject Rights. Taking into account the nature of the Services, Vercel offers Customer
certain controls as described in Sections 2.1 and 6.2 that Customer may elect to use to comply
with its obligations towards Data Subjects. Should a Data Subject contact Vercel with regard to
correction or deletion of its Personal Data, Vercel will use commercially reasonable efforts to
forward such requests to Customer; provided, however, that Customer shall remain responsible
for handling and responding to any Data Subject requests as required by Data Protection
Legislation.

9. Optional Security. Vercel makes available a number of security features and functionalities that
Customer may elect to use. Customer is responsible for (a) implementing the measures
described in Section 6.2, as appropriate, (b) properly configuring the Services, (c) using the
controls available in connection with the Services (including the security controls) to allow
Customer to restore the availability and access to Customer Data in a timely manner in the event
of a physical or technical incident (e.g. backups and routine archiving of Customer Data), and
(d) taking such steps as Customer considers adequate to maintain appropriate security,
protection, and deletion of Customer Data, which includes use of encryption technology to
protect Customer Data from unauthorized access and measures to control access rights to
Customer Data.


10.1. Security Incident. Vercel will (a) notify Customer of a Security Incident without undue delay
after becoming aware of the Security Incident, and b) take reasonable steps to mitigate the
effects and to minimize any damage resulting from the Security Incident.

10.2. Vercel Assistance. To assist Customer in relation to any Personal Data breach
notifications Customer is required to make under GDPR, Vercel will include in the notification under section 10.1(a) such information about the Security Incident as Vercel is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Vercel, and any restrictions on disclosing the information, such as confidentiality.

10.3. **Unsuccessful Security Incidents.** Customer agrees that:

a. An unsuccessful Security Incident will not be subject to this Section 10. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of Vercel’s equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful login attempts, denial of service attacks, packet sniffing (other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

b. Vercel’s obligation to report or respond to a Security Incident under this Section 10 is not and will not be construed as an acknowledgement by Vercel of any fault or liability of Vercel with respect to the Security Incident.

10.4. **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer’s administrators by any means Vercel selects, including via email. It is Customer’s sole responsibility to ensure Customer’s administrators maintain accurate contact information on the Vercel team console and secure transmission at all times.

11. **Assistance and Audits.**

11.1. **Data Protection Impact Assessment.** Taking into account the nature of the Processing and the information available to Vercel, Vercel will provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer will be responsible for any costs and expenses arising from any such assistance by Vercel, unless prohibited by applicable law.

11.2. **Prior Consultation.** Taking into account the nature of the Processing and the information available to Vercel, Vercel will provide Customer with reasonable cooperation and assistance with respect to Customer’s cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer will be responsible for any costs and expenses arising from any such assistance by Vercel, unless prohibited by applicable law.

11.3. **Inspection.** Upon Customer’s reasonable request, and no more than once per calendar year, Vercel will make available for Customer’s inspection and audit, copies of certifications, records or reports demonstrating Vercel’s compliance with this DPA. In the event that Customer reasonably determines that it must inspect Vercel’s premises or equipment for purposes of this DPA, then no more than once per calendar year, any audits described in this Section 11 will be conducted, at Customer’s expense, through an independent third-party auditor (“Independent Auditor”) designated by Customer, during normal business hours, and upon twenty (20) days’ prior written notice to Vercel; provided, however, that in the event of a Security Incident, the twenty-day notice requirement will be waived and the parties will agree upon a reasonable, mutually agreeable time. Any inspection will be of reasonable duration and will not unreasonably interfere with Vercel’s
day-to-day operations. All Independent Auditors are required to enter into a non-disclosure agreement containing confidentiality provisions reasonably acceptable to Vercel and intended to protect Vercel’s and its customers’ confidential and proprietary information. Customer will make (and ensure that any Independent Auditor makes) reasonable endeavors to avoid causing any damage, injury or disruption to Vercel’s premises, equipment, personnel and business in the course of such an audit or inspection. To the extent that Customer or any Independent Auditor causes any damage, injury or disruption to the Vercel’s premises, equipment, personnel and business in the course of such an audit or inspection, Customer will be solely responsible for any costs associated therewith.

12. Transfers of Personal Data.

12.1. Application of Standard Contractual Clauses. The EU Controller to Processor Standard Contractual Clause Agreement (“Standard Contractual Clauses”), attached hereto as Annex 2, will apply to Customer Data that is transferred outside the EEA or the United Kingdom, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data. The Standard Contractual Clauses will not apply (a) to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA or the United Kingdom or (b) if Vercel has adopted, at its sole discretion, Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of Personal Data outside the EEA or the United Kingdom. By executing this DPA, Vercel and Customer agree to be bound by the obligations set forth in the Standard Contractual Clauses. The parties agree that (i) purely for the purposes of the descriptions in the Standard Contractual Clauses, Vercel will be deemed the “data importer” and Customer will be deemed the “data exporter” (notwithstanding that Customer itself may be located outside the EEA or UK and/or be acting as a processor on behalf of third party controllers); (ii) Annex 1 hereto will serve as Appendix 2 to the Standard Contractual Clauses; and (iii) if and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict. In the event that the Standard Contractual Clauses are modified or amended by the European Commission, the parties agree to be bound by the amended clauses.

12.2. Government Requests. As of the date of Vercel’s signature to this DPA, Vercel has not received any requests under Section 702 of the Foreign Intelligence Surveillance Act or Executive Order 12333.

13. Termination of the DPA. This DPA will continue in force until the termination of the Services Agreement (the “Termination Date”).

14. Return or Deletion of Customer Data. Up to the Termination Date, Customer will continue to have the ability to retrieve or delete Customer Data in accordance with Section 2.1 and this Section. For 90 days following the Termination Date, Customer may retrieve or delete any remaining Customer Data from the Services, subject to the terms and conditions set out in the Services Agreement, unless prohibited by law or the order of a governmental or regulatory body or it could subject Vercel or its Affiliates to liability. No later than the end of this 90-day period, Customer will close all Vercel accounts. Vercel will delete Customer Data when requested by Customer by using the Service controls provided for this purpose by Vercel.

15. Duties to Inform. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Vercel, Vercel will inform Customer without undue delay. Vercel will, without undue delay, notify all
relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer’s property and area of responsibility and that Customer Data is at Customer’s sole disposition.

16. **Liability.** The total liability of Vercel (and its respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the lesser of: (a) the limitation of liability for aggregate or direct damages set forth in the Services Agreement; and (b) one hundred thousand dollars.

17. **Choice of Law.** Without prejudice to any requirements under the GDPR, or clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the EU Standard Contractual Clause Agreement, the parties hereby submit to the choice of venue and jurisdiction stipulated in the Services Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; provided, however, that the parties agree that this DPA shall be governed by the laws of Ireland.

18. **Entire Agreement; Conflict.** Except as amended by this DPA, the Services Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Services Agreement and this DPA, the terms of this DPA will control.

The parties’ authorized signatories have duly executed this Agreement:

**CUSTOMER**

Signature: .................................................................................................................................

Print Name: ..............................................................................................................................

Title: ........................................................................................................................................

Customer Legal Name: ............................................................................................................

Date: ........................................................................................................................................

**Vercel Inc.**

Signature: .................................................................................................................................

Chris Leishman
Chief Operating Officer
March 30, 2021
Annex 1
Vercel Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Services Agreement.

1. **Information Security Program.** Vercel will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Vercel Network, and (c) minimize security risks, including through risk assessment and regular testing. Vercel will appoint one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1. **Network Security.** The Vercel Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. Vercel will maintain access controls and policies to manage what access is allowed to the Vercel Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Vercel will maintain corrective action and incident response plans to respond to potential security threats.

2. **Continued Evaluation.** Vercel will conduct periodic reviews of the security of its Vercel Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Vercel will continually evaluate the security of its Vercel Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by periodic reviews.
Annex 2
Standard Contractual Clauses (Controller to Processor)

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 [This opening recital is deleted if these Clauses are not governed by the law of a member state of the EEA (e.g. on Brexit.)].

Name of the data exporting organization: .................................................................

Address: ........................................................................................................................

.................................................................................................................................

.................................................................................................................................

Tel.: ......................................; fax: ......................................; e-mail: ............................

Other information needed to identify the organization:

........................................................................................................................................

(the data exporter)

And

Name of the data importing organization: Vercel Inc.

Address: 548 Market St #61948

San Francisco, CA 94104

United States

Tel.: +1 (951) 383-6898  ; fax: n/a  ; e-mail: privacy@vercel.com

Other information needed to identify the organization:

........................................................................................................................................

(the data importer)

each a “party”; together “the parties”,
HAVEN 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.

Background

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and
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; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.]

(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; [If these Clauses are not governed by the law of a Member State, the words "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" are deleted.]

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 subprocessor 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 subprocessor 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; [If these Clauses are not governed by the law of a Member State, the words “within the meaning of Directive 95/46/EC” are deleted.]

(g) to forward any notification received from the data importer or any subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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
Clause 5: Obligations of the data importer

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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data importer 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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: **Subprocessing**

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor’s obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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.

4. The data exporter shall keep a list of subprocessing 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 subprocessor 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 subprocessor 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.
**On behalf of the data exporter:**
[Populated with details of, and deemed signed on behalf of, the data exporter.]

Name (written out in full): ...........................................................................................................

Position: .................................................................................................................................

Address: ................................................................................................................................
.............................................................................................................................................
.............................................................................................................................................
.............................................................................................................................................

Other information necessary in order for the contract to be binding (if any):

Signature: ...............................................................................................................................

---

**On behalf of the data importer:**
[Populated with details of, and deemed signed on behalf of, the data importer.]

Name (written out in full): **Chris Leishman**

Position: **Chief Operating Officer**

Address: 548 Market St #61948

San Francisco, CA 94104

United States

Other information necessary in order for the contract to be binding (if any):

Signature: ...............................................................................................................................
Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. Defined terms have the meaning set forth in the DPA.

Data exporter
The data exporter is:

.......................................................... ..........................................................
.......................................................... ..........................................................
.......................................................... ..........................................................

Data importer
The data importer is:

Vercel, Inc.

Data subjects
The personal data transferred concern the following categories of data subjects:

Customer’s customers, employees, suppliers and end-users.

Categories of data
The personal data transferred concern the following categories of data:

Customer Data as defined in the DPA.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

None

Processing operations
The personal data transferred will be subject to the following basic processing activities:

Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

DATA EXPORTER
[Populated with details of, and deemed to be signed on behalf of, the data exporter:]

Name: ..................................................................................................................

Authorised Signature: .........................................................................................

DATA IMPORTER
[Populated with details of, and deemed to be signed on behalf of, the data importer:]

Name: Chris Leishman

Authorised Signature: .........................................................................................
Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

See Annex 1 to the DPA.