Data Processing Agreement

Last Updated March 30, 2023

On this page

1. Introduction

This Data Processing Addendum ("Addendum") is entered into and is supplemental to, and made pursuant to, 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") as of the effective date of such Agreement ("Effective Date") and is by and between Vercel Inc., a Delaware corporation ("Vercel"), and the Customer that executed the Agreement. This Addendum applies to Vercel's Processing of Personal Data under 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 Addendum only, and except where indicated otherwise, the term "Customer" shall include Customer and Affiliates.

This Addendum shall become legally binding upon Customer entering into the Agreement.

2. Definitions

Any terms used in this Addendum and not defined will have the meanings given to them in the applicable 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Protection Laws" means all applicable privacy and data protection laws and regulations and in each case, as amended, superseded, or replaced from time to time, including, without limitation, the EU General Data Protection Regulation (EU) 2016/679 ("GDPR"); the United Kingdom Data Protection Act 2018; the California Consumer Privacy Act of 2018 ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and the Australian Privacy Principles and the Australian Privacy Act (1988).
c. "Contact Data" means the Personal Data that Vercel Processes as a controller, such as account information, payment information, and event attendee information.
d. "Customer Data" means the Personal Data that Vercel Processes on behalf of Customer.
e. "Data Subject" means the identified or identifiable natural person who is the subject of Personal Data or the meaning as set forth in Applicable Data Protection Laws, including similar terms, such as "Consumer" as used in the CCPA.
f. "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 and including all "processing" as defined in any Applicable Data Protection Laws.
g. "Personal Data" means "personal data", "personal information", "personally identifiable information" or similar information defined in and governed by Applicable Data

Protection Laws.

h. "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 Processed by Vercel and/or its Subprocessors in connection with the provision of Services. 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.
i. "Service-Generated Data" means usage data and metadata that is generated through the use of the Services, including data generated through the use of Support Services. This Addendum applies to Service-Generated Data to the extent Service-Generated Data constitutes Personal Data.
j. "Services" means collectively the PaaS and the Audit and Training Services, each as defined in the Agreement.
k. "Subprocessor" means any third-party authorized by Vercel to Process Customer Data in assistance with fulfilling its obligations with respect to providing Services under the Agreement or this Addendum.

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 remain in effect until, and automatically terminate upon, deletion of Customer Data as described in this Addendum.

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 (or processor) and Vercel is a processor. Vercel will process Customer Data under and in accordance with Customer's instructions (on behalf of the controller) as outlined in Section 6 (Role and Scope of Processing).
b. Vercel as Controller. To the extent that any Service-Generated Data is considered Personal Data and as to any Contact 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

6. Role and Scope of the Processing

a. **Customer Responsibilities.** Customer is solely responsible for obtaining and maintaining all the necessary consents prior to accessing, storing, uploading, processing, or storing Customer Data in the Service. Customer has provided, and will continue to provide, all notices and has obtained, and will continue to obtain, all consents, permissions, and rights necessary under applicable laws, including Applicable Data Protection Laws, for Vercel to lawfully process Customer Data for the purposes contemplated by the Agreement. Customer has complied with all applicable laws, rules, and regulations, including Applicable Data Protection Laws, in the collection and provision to Vercel and its Subprocessors of such Customer Data.
b. **Customer Instructions.** Vercel will Process Customer Data only in accordance with Customer's documented, lawful instructions on behalf of the controller, except to the extent required by Applicable Data Protection Laws to which Vercel is subject or where Vercel becomes aware or believes that Customer's instructions violate Applicable Data Protection Laws, in which case Vercel will notify Customer. 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; (b) to perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement; and (c) does not conflict with the instructions given to the Customer by the controller to Process Customer Data.

7. Subprocessing

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 to the extent applicable to the nature of the services provided by such Subprocessor; 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://security.vercel.com, and may be updated by Vercel from time to time in accordance with this Addendum.
c. Customer must email privacy@vercel.com or other method as communicated by Vercel to Customer in the future, to subscribe to notice of new Subprocessors that will be engaged. Vercel will notify Customer by updating the list of Subprocessors and, if Customer has subscribed to notices as set forth in the preceding sentence, via email. 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

remain liable to pay any committed fees in an order form, order, statement of work or other similar ordering document.

8. Security

a. **Security Measures.** 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**"). For more information on Vercel's security measures please see our Security FAQs at https://vercel.com/security.
b. **Customer Responsibility.**
    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 provide a level of security appropriate to the risk in respect of the Customer Data and that they 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 notice to Customer will describe, to the extent possible, (a) the details of the Security Incident as known or as reasonable requested by Customer, and (b) the steps taken, deemed necessary and reasonable by Vercel, to mitigate the potential risks, to the extent that the remediation is within Vercel's reasonable control. 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 acknowledgment by Vercel of any fault or liability with respect to the Security Incident. These obligations will not apply to Security Incidents to the extent they are caused by Customer.

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 Laws 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. Such audits (e.g., SOC 2 Type 2) 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 Schedule 2.
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.

10. Impact Assessments and Consultations

Vercel will provide reasonable cooperation to Customer, to the extent Customer does not otherwise have access to the relevant information and such information is available to Vercel, 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 as required by 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 the Processing of 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. Customers may delete or export Customer Data at any time while using the Services in a manner consistent with the functionality of the Service. Termination or expiration of the Agreement serves as instruction for Vercel to delete all Customer Data within a commercially reasonable timeframe.
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. Notwithstanding

Data, Vercel's primary processing facilities are in the United States. Notwithstanding the foregoing, Customer acknowledges that Vercel may in connection with the provision of Services, need to transfer and process Customer Data to and in the United States and anywhere else in the world where Vercel or its Subprocessors maintain data processing operations. Vercel will ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this Addendum.

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.

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. **Service-Generated Data and Contact Data.** Vercel will process Service-Generated Data and Contact 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 and disclosures in accordance with the Agreement and/or as compelled by applicable laws.
b. **Service-Generated Data and Contact Data.** Personal Data contained in Service-Generated Data and/or Contact Data will be subject to the following processing activities by Vercel: Vercel may use Service-Generated Data and/or Contact Data to operate, improve and support the Services, to provide marketing and service-related messages 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 Customer Data in accordance with sections 3 and 12 of this Addendum.
b. **Service-Generated Data and Contact Data.** Upon termination of the Agreement, Vercel may retain, use, and disclose Service-Generated Data and/or Contact Data for the purposes set forth above in Section 2.b (Service-Generated Data and Contact Data) of this Schedule 1, subject to the confidentiality obligations set forth in the Agreement. Vercel will anonymize or delete Personal Data contained within Service-Generated Data and/or Contact Data when Vercel no longer requires it for the purpose set forth in Section 2.b (Service-Generated Data and/or Contact Data) of this Schedule 1.

4. Categories of Data Subjects

a. **Customer Data.** Individuals whose Personal Data is included in Customer Data.
b. **Service-Generated Data and Contact Data.** Customer's authorized users with access to a Vercel account, customers, suppliers, and end users.

5. Categories of Personal 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.

1. Measures of pseudonymization and encryption of personal data.

Vercel maintains Customer Data in an encrypted format at rest using Advanced Encryption Standard (AES-256) and in transit (TLS 1.2 or higher).

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 Subprocessors to sign confidentiality provisions that are substantially similar to those contained in Vercel's Customer agreements. All employees (and contractors) are bound by Vercel's internal policies regarding maintaining the confidentiality of Customer Data and are contractually obligated to comply with these obligations.

The Services operate on Amazon Web Services ("**AWS**"), Microsoft Azure ("**Azure**"), and

Google Cloud Platform ("GCP") and are protected by the security and environmental controls of Amazon and Google, respectively. 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.

Vercel performs regular backups of Customer Data, which is hosted in AWS, Microsoft Azure, and GCP data centers. Backups are globally replicated for resiliency against regional disasters and periodically tested by the Vercel engineering team.

Employees complete mandatory training annually, which covers privacy and data protection, confidentiality, social engineering, password policies, and information security.

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 GCP data centers. Backups are retained redundantly across multiple availability zones and encrypted in transit and at rest.

Vercel has a business continuity and disaster recovery plan that incorporates input from periodic risk assessments, vulnerability scanning, and threat analysis.

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 (e.g., SOC 2 Type 2, penetration testing, and vulnerability scanning).

Vercel's security governance program covers: Policies and Procedures, Asset Management, Access Management, Data Handling, Encryption, Logging & Monitoring, Password Management, Personnel Security, Resiliency, Responsible Disclosure, Risk Assessment, Vendor Risk Management, Vulnerability, SDLC, Incident Response, Business Continuity & Crisis Management, Acceptable Use and Code of Conduct. Information security policies and standards are reviewed and approved by management at least annually and are made available to all employees.

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.

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. Employee access to Customer Data is promptly removed upon role change or termination.

Vercel uses commercially reasonable practices to identify and authenticate users who attempt to access Vercel systems.

6. Measures for the protection of data during transmission.

Customer Data is encrypted when in transit between Customer and the Vercel Services.

7. Measures for the protection of data during storage.

Customer Data is stored encrypted using AES-256. Vercel uses AWS Key Management System ("KMS") to encrypt data in our infrastructure. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect keys that cannot be retrieved from the service by anyone or transmitted beyond the AWS regions where they were created. AWS log-in credentials and private keys generated by the Service are for Vercel's internal use only.

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

Vercel is a remote-first organization with limited physical presence globally. As needed, physical security controls for office space are inherited from our co-working office provider, which manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security.

The Services operate on AWS, Microsoft, and GCP and are protected by the security and environmental controls of Amazon, Microsoft, and Google, respectively.

Detailed information about AWS security is available at:

- https://aws.amazon.com/security/
- 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 GCP 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.

User activity metrics are available to Customers within the Services. For further information, visit https://vercel.com/docs/observability/activity-log.

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; and (b) annual penetration testing by independent third parties.

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 to provide independent feedback on the operating effectiveness of the information security program (e.g., SOC 2 Type 2, penetration testing, and vulnerability scanning).

Vercel's security governance program covers Policies and Procedures, Asset Management, Access Management, Data Handling, Encryption, Logging & Monitoring, Password Management, Personnel Security, Resiliency, Responsible Disclosure, Risk Assessment, Vendor Risk Management, Vulnerability, SDLC, Incident Response, Business Continuity & Crisis Management, Acceptable Use and Code of Conduct. Information security policies and standards are reviewed and approved by management at least annually and are made available to all employees.

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.

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

Vercel conducts various third-party audits to attest to various frameworks including SOC

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

AWS, Azure, and GCP have achieved: SOC 1, 2, and 3; ISO 27001, 27017, 27018, 27701, and 9001; Cloud Security Alliance Security, Trust, Assurance and Risk (CSA STAR); FedRAMP; and use FIPS 140-2 validated cryptographic modules, in addition to meeting compliance standards for many other legal, security, and privacy frameworks. Further information about these providers' security practices can be found on their respective websites.

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 Service-Generated Data that Vercel collects and to ensure that the Vercel Services are 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.

Vercel has a process that allows individuals to exercise their privacy rights, as described in Vercel's Privacy Notice available at https://vercel.com/legal/privacy-policy.

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. Customers have the ability to delete Customer Data via the self-service functionality of the Services. Vercel will, within a commercially reasonable timeframe after request by Customer following the termination or expiration of the Agreement, delete all Customer Data from Vercel's systems, unless required by 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://security.vercel.com), 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 self-service functionality that allows Customers to delete and suppress their Customer Data.

Vercel specifies in the Addendum that it will provide assistance to such Customer as may reasonably be required 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

Schedule 3: Cross Border Data Transfer Mechanism

1. Definitions

a. "Standard Contractual Clauses" means the 2021 Standard Contractual Clauses approved by the European Commission in decision 2021/914.
b. "UK IDTA" means the UK international data transfer addendum (Schedule 5).

2. UK IDTA

For data transfers from the United Kingdom, the UK IDTA will be deemed entered into (and incorporated into this Addendum by reference) together with the Standard Contractual Clauses as set forth in Section 3 of this Schedule below.

3. The 2021 Standard Contractual Clauses

For data transfers from the EEA, the UK, and Switzerland that are subject to the Standard Contractual Clauses, the Standard Contractual Clauses will apply in the following manner:

a. Module One (Controller to Controller) will apply where Customer is a controller of Service-Generated Data and/or Contact Data and Vercel is a controller of Service-Generated Data and/or Contact Data.

b. Module Two (Controller to Processor) will apply where Customer is a controller of Service-Generated Data and/or Contact Data and Vercel is a processor of Service-Generated Data and/or Contact Data.

c. Module Three (Processor to Processor) will apply where Customer is a processor of Service-Generated Data and/or Contact Data and Vercel is a processor of Service-Generated Data and/or Contact 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 Subprocessor 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 - 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 Subprocessors, the subject matter, nature, and duration of the processing is outlined at https://security.vercel.com.

Schedule 4: Jurisdiction Specific Terms

1. California

a. The definition of "Applicable Data Protection Laws" 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 with the Customer as the business.
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 Service-Generated Data is considered Personal Data and/or as to Contact Data, pursuant 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.

h. Vercel implements and maintains reasonable security and privacy practices appropriate to the nature of the personal information that it processes as set forth in section 8 of this Addendum.

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

Schedule 5: UK IDTA

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	the Effective Date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See the Agreement	Full legal name: Vercel Inc. Trading name (if different): n/a Main address (if a company registered address): 440 N Barranca Ave #4133, Covina, CA 91723 Official registration number (if any) (company number or similar identifier): Delaware, 5857312
Key Contact	See the Agreement	Contact details including email: privacy@vercel.com
Signature (if required for the purposes of Section 2)	By entering into the Agreement, Exporter is deemed to have signed this Addendum.	By entering into the Agreement, Importer is deemed to have signed this Addendum.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this

	Addendum: See Schedule 3, Section 3

Personal data received from the Importer may be combined with personal data collected by the Exporter.

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A:	List of Parties: See Table 1
Annex 1B:	Description of Transfer: See Schedule 1
Annex II:	Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 2
Annex III:	List of Sub processors (Modules 2 and 3 only): See https://security.vercel.com

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the

following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced

legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's

processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards

writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws; The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or
b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Company

About

Blog

Careers

Changelog

Contact Us

Customers

Events

Partners

Shipped

Privacy Policy

Legal

Social

GitHub

LinkedIn

Twitter

YouTube

All systems normal.