Data Processing Addendum

Last dated March 31, 2026
Effective date March 31, 2026

1. Introduction

This Data Processing Addendum ("**Addendum**") forms part of Vercel Enterprise Terms and Conditions or other agreement between Vercel and Customer for the provision of the Vercel Services (the "**Agreement**"). This Addendum, effective date of such agreement ("**Effective Date**") and any Agreement between Vercel, a Delaware corporation ("**Vercel**") and the Customer that executed the Agreement ("**Customer**") governs the Processing of Personal Data in connection with the Vercel Services. Capitalized terms not defined herein shall have the meanings set forth in the Agreement.

Customer enters into this Addendum on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if any. For the purposes of this Addendum only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

The Addendum shall become legally binding upon the Effective Date of the Agreement or upon execution of this Addendum.

2. Definitions

Any capitalized term in this Addendum and not defined will have the meanings given to it in the Applicable Data Protection Laws.

- **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" means ownership of or the right to control 50% or more of the voting securities of the subject entity.
- **"Applicable Data Protection Laws"** means all applicable privacy and data protection laws and regulations and/or rules to such laws as amended, superseded or replaced from time to time, including, to the extent applicable, the European Data Protection Regulations ("EU DPR") ("**EDPR**"), the United Kingdom Data Protection Regulations ("**UK DPR**"), the Swiss Data Protection Laws ("**Swiss DPL**"), the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**") and the California Consumer Privacy Act and the Regulations thereto ("**CCPA**").
- **"Contact Data"** means the Personal Data that Vercel Processes as a controller, including Customer personal information, passport information and travel sensitive information.
- **"Controller"** will have the following meaning (as applicable): (a) the meaning ascribed to it in the EDPR; (b) the meaning ascribed to it in the UK DPR; (c) the meaning given to "business" under Applicable Data Protection Laws;
- **"Customer Data"** means the Personal Data or Non-Contact Vercel Service Provisioning Data Processed by Vercel on Customer's behalf.
- **"Data Subject"** means the identified or identifiable natural person to which the Personal Data relates or any "consumer" or "household" as that term is defined in Applicable Data Protection Laws, including (where such an "Consumer" is so defined or recognized) a Data Subject.
- **"Processor"** means any person or, as of Applicable Data Protection Laws, an "service provider" or "contractor" or "processor" or "sub-processor" or "processor" or "sub-processor" or "service provider" or "contractor" or any other similar term, including (where such a "Consumer" is so defined or recognized) a Processor.
- **"Personal Data"** means any information relating to an identified or identifiable natural person, or "personal information" or "personal data" or "personally identifiable information" or any equivalent or similar term in Applicable Data Protection Laws, including (where such a "Consumer" is so defined or recognized) Personal Data.
- **"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, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "Process", "Processes" and "Processed" will be construed accordingly.
- **"Sub-Processor"** means any Processor engaged by Vercel or any member of Vercel's group of companies or any third party appointed by or on behalf of Vercel to Process Personal Data on behalf of any Customer Data Controller.
- **"Supervisory Authority"** means any third party authorized by Vercel to Process Customer Data under the Agreement, including (where such a "Consumer" is so defined or recognized) Data Subject.

3. General; Termination

1. 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 the Agreement and this Addendum, the terms of this Addendum will govern.
2. Any liability arising under this Addendum are subject to the limitations of liability in the Agreement.
3. 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.
4. This Addendum will terminate in effect until, and automatically terminate upon, deletion of Customer Data by Processor in accordance herein.

4. Relationship of the Parties

1. **Vercel as Processor.** The parties acknowledge and agree that with regard to the Processing of Customer Data for Customer purposes vis-a-vis Enterprise or the plans, Customer may act either as a Controller or Processor, and Vercel may act as a Processor. Vercel processes Customer Data only when in accordance with Customer's instructions, on behalf of the Controller as outlined in Section 6 Africa also Scope of Processing. Vercel's EDPR roles are as a Processor.
2. **Vercel as Controller.** To the extent that any Vercel Personnel Contact Data is considered Personal Data and to the as Contact Data, Vercel is the Controller of Contact Data and Customer Data. Vercel Contact Data is Processed in accordance with Privacy Notice. For the avoidance of doubt, Schedule 1 does not apply when Vercel Processes Contact Data as a Controller.

5. Compliance with Law

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

6. Role and Scope of the Processing

1. **Customer Responsibilities.** Customer is solely responsible for obtaining and maintaining all the necessary consents prior to establishing, storing, processing, or sending Customer Data or the Services. Customer has provided and will continue to provide all notice and has obtained and will continue to maintain all consents, permissions, and rights necessary under Applicable Data Protection Laws, lawful instructions, and lawful basis of Processing, and Vercel's Processing for the purposes contemplated by the Agreement. Customer has complied with and will continue to comply with all laws, including Applicable Data Protection Laws, in the collection and provision to Vercel and its Subprocessors of any Customer Data.
2. **Processing Instructions.** Vercel will Process Customer Data only in accordance with Customer's documented lawful instructions, except to the extent required otherwise by Applicable Data Protection Laws. The parties agree that the Agreement, Customer has complied with and will continue to comply with all laws, including Applicable Data Protection Laws, in the collection and provision to Vercel and its Subprocessors of any Customer Data.
3. **Processing Purposes.** Vercel will Process Customer Data only in accordance with Customer's documented lawful instructions, except to the extent required otherwise by Applicable Data Protection Laws. The parties agree that the Agreement, Customer has complied with and will continue to comply with all laws, including Applicable Data Protection Laws, in the collection and provision to Vercel and its Subprocessors of any Customer Data.
4. **Prohibited Data.** Customer will not provide (or cause to be provided) any Sensitive Data or vice versa Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Customer shall not Process, or permit any Data Subjects to Process, Sensitive Data in connection with the Services.
5. **Customer Processing.** Customer agrees that it is solely responsible for its Processing of Personal Data in and related Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and that such Customer Processing of Customer Data will comply with the requirements of Applicable Data Protection Laws.

7. Subprocessing

1. Customer authorizes Vercel to Process Data to use Affiliates as Subprocessors, and generally authorizes Vercel to engage Subprocessors to Process Customer Data. Vercel's Affiliates shall abide by the same obligations as Vercel and Subprocessors. 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. Vercel shall remain responsible for the obligations of the Addendum and for any acts or omissions of the Subprocessor that cause Vercel to breach any of its obligations under this Addendum.
2. **List of Subprocessors.** Customer agrees that Vercel may engage Subprocessors available at https://vercel.com/sub-processors. Vercel may add Subprocessors from time to time in accordance with this Addendum.
3. **Notice of Subprocessors.** Customer agrees that Vercel may notify Customer of any Subprocessors to be added by notifying Customer at their Dashboard. Customer may object to Vercel's use of a Subprocessor by notifying Vercel promptly in writing within ten (10) business days after receipt of Vercel's notice. If Customer reasonably objects to the use of a Subprocessor, Customer shall notify Vercel in writing of its specific objections within ten (10) days after receipt of Vercel's notice, and the parties will then promptly and reasonably attempt to resolve the matter. If the parties are not able to mutually agree to a resolution of such concern, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience with respect to the Services affected by the new Subprocessor, in which case Customer will cease its use of the Services affected by such Subprocessor.

8. Security

1. **Security Measures.** Vercel will implement and maintain technical and organizational measures in relation to the Processing of Customer Data to Vercel's Security and to preserve the security and confidentiality of the Customer Data, in accordance with Vercel's security standards referenced in the Agreement ("**Vercel Security Standards**") and Vercel's Information Security Handbook (which are Vercel's Security Measures and Security Documentation).
2. **Customer Responsibility.**
   - Customer is responsible for reviewing the information made available by Vercel relating to data security and making an independent determination to Customer that the Vercel 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 to reflect the current state of art, the costs of implementation and the nature, scope, context and purposes of the Processing of Customer Personal Data and to implement any measures to Vercel whichever is sooner and as of the Effective Date.
   - Customer agrees that, without limitation of its own 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 to connect to the Services, and (d) securing the Customer Data at Customer rest.
3. **Security Incident.** To the extent required by Applicable Data Protection Laws, Vercel will notify Customer of any Security Incident without undue delay or Customer without initial delay after becoming aware of a Security Incident, in giving such notice requested by law enforcement and/or in light of Vercel's ongoing investigation of a Security Incident. Vercel will promptly and reasonably carry out coordinate an initial delay, from notice to Customer will deadline, to the extent possible, to the details of the Security Incident as known or as reasonable anticipated by Vercel at the time of notice, and thereafter as Vercel shall reasonably be required, to mitigate the potential risks, to the extent that in Vercel's sole judgment, Customer and Vercel shall cooperate in good faith to undertake appropriate 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 the Section 8c 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 Incidents to the extent that 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.

1. **Vercel's Audit Program.** Vercel uses external auditors to verify the adequacy of its security measures with respect to the processing of Customer Data. Such audits are: (a) at least annually; (b) conducted in accordance with standards recognized by independent third-party security organizations; (c) performed at Vercel's expense by independent third-party security professionals; and (d) generate a report or other documentation summarizing the results of the audit ("**Audit Report**"). Upon Customer's written request and subject to appropriate confidentiality and security, Vercel will make available to Customer a copy of Vercel's most recent Audit Report. Customer agrees that any Audit Report provided by Vercel shall be deemed Vercel's Confidential Information.
2. **Customer Audit Rights.**

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 any data protection impact assessment or relevant prior consultation Customer is cooperate only if such reasonable cooperation will impact Vercel to assign sufficient resources to such. Such cooperation will require submission as requested by Applicable Data Protection Laws.

11. Data Subject Requests

Vercel will inform Customer's request Vercel and if Customer's expected process 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 ("**Data Subject Requests**"), including, without limitation, access, rectification, restriction, deletion or portability of Personal Data, to the extent permitted by law. Customer is solely responsible for responding to any Data Subject Requests which relate to any use of the Vercel Services functionality of the Services. If Vercel receives a request from a Data Subject in relation to Customer Data, Vercel will advise the Data Subject to submit his or her request to Customer, and Customer will be responsible for responding to any such request.

12. Return or Deletion of Customer Data

1. Customers may delete a saved Customer Data at any time while using the Services in a manner consistent with the functionality of the Services. Termination of the Agreement will result in deletion of Customer Data from Vercel's Customer Data within a commercially reasonable timeline.
2. Upon termination of the Agreement, Vercel will delete all Customer Data and Customer Data if requested by law and such data will remain subject to the requirements of the Addendum.

13. International Provisions

1. **Processing in the United States.** Customer acknowledges that, as of the Effective Date, Vercel maintains a data center in the United States. Vercel's Sub-Processing the foregoing Customer acknowledges that Vercel may in its sole discretion, Process Customer Data in the United States and anywhere in Customer Data is stored in the United States and anywhere else in the world where Vercel, its Affiliates or Subprocessors maintain data processing operations. Vercel shall at all times ensure compliance by such Subprocessors with the obligations of Vercel under this Addendum.
2. **Cross-Border Data Transfer Mechanisms.** To the extent that Customer's use of the Services requires the transfer of Personal Data from the EEA, UK or Switzerland to a Third Country or to a jurisdiction for which the European Commission, the Swiss Federal Council or the UK Government (as applicable) has not issued a determination that it provides an adequate level of protection in respect of Personal Data, the parties shall be deemed to have entered into the Standard Contractual Clauses, the Swiss Clauses or the UK Addendum (the "**Transfer Mechanisms**"), the terms and conditions of Schedule 2 (Cross-Border Transfer Mechanisms) with 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 to and user information with such Subprocessors. Vercel will not share and Customer Data with third parties for third parties' and business interests.

1. **Customer Data.** Vercel will process Customer Data as a processor in accordance with Vercel's Data Protection as outlined in Applicable Data Protection Laws and as outlined in this Addendum.
2. **Service Generated Data and Contact Data.** Vercel will process Service Generated Data and Contact Data as a Controller in accordance with Section 4 Vercel as Controller of Information.

2. Processing Activities

1. **Customer Data.** Customer Data will be subject to the following basic processing activities: (a) storage and other Processing necessary to provide the Services in accordance with Agreement; (b) transmission.
2. **Service Generated Data and Contact Data.** Personal Data contained in Service Generated Data and Contact Data will be subject to the following basic processing activities by Vercel: Vercel may use the Service Generated Data and Contact Data to operate, improve and support the Services, to provide marketing and service information to Customer, to make recommendations, and 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 the period is as follows:

1. **Customer Data.** Prior to the termination of the Agreement, Vercel will Process Customer Data in accordance with sections 5 and 12 of the Addendum. Following termination of the Agreement, Vercel will Process Customer Data, thereafter, Vercel retains, uses and disclosure Service Generated Data and Contact Data for the purposes set forth above in Section Service Generated Data and Contact Data, subject to Vercel's compliance with Applicable Data Protection Laws and Section 4 of the Agreement. Vercel will anonymize or delete Personal Data contained within Service Generated Data and/or Contact Data when Vercel no longer requires the Personal Data for the purposes for which the Personal Data was collected.
2. **Service Generated Data and Contact Data.** Vercel processes Service Generated Data and Contact Data, which is hosted in AWS.

4. Categories of Data Subjects

1. **Customer Data.** Customers are authorized Vercel including sensitive data or special categories of data under Applicable Data Protection Laws.
2. **Service Generated Data and Contact Data.** Customer data is not contained in Service Generated Data and Contact Data.

5. Categories of Personal Data

1. **Customer Data.** The categories of Customer Data are: any Customer Data that Customer elects to Process in the Services provided to Customer and in connection with the performance of the Services, to the extent of or similar to, exclusively determined and controlled by the Customer, such as IP address and other Personal Data elements.
2. **Service Generated Data and Contact Data.** Vercel processes Personal Data within Service Generated Data and Contact Data, such as name, email address, phone number, IP address, and payment information associated with Support Services.

6. Sensitive Data or Special Categories of Data

1. **Customer Data.** Customers are authorized Vercel including sensitive data or special categories of data under Applicable Data Protection Laws.
2. **Service Generated Data and Contact Data.** Sensitive data is not contained in Service Generated Data and Contact 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 to protect Customer Data.

1. Measures of pseudonymization and encryption of personal data.

Vercel encrypts all Customer Data in an encrypted format in transit. Vercel encrypts Customer Data at rest using AES-256 and is hosted GCS in US region.

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

Vercel's Customer agreements contain strict confidentiality obligations. Additionally, Vercel requires every subprocessor to sign a Data Processing Addendum containing 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 business information with customers and with these obligations.

The Services operate on Amazon Web Services ("**AWS**"), Microsoft Azure ("**Azure**"), and Google Cloud Platform ("**GCP**") infrastructure. This infrastructure provides environmental controls of Amazon and Google respectively. The infrastructure for the Vercel Services uses multi-zone, fault-independent AWS availability zones in Azure and GCP regions. Vercel's Services are designed to automatically detect failures and processes to maintain high availability of the Services.

Vercel performs regular backups of Customer Data, which is hosted in AWS, Azure, and GCP. Vercel's Services are designed to be fault tolerant and to withstand against logical disasters and particularly limited by Vercel engineering team.

Employees complete mandatory training annually, which covers privacy and data protections, confidentiality, social engineering, password policy, and incident response.

3. Measures for ensuring the ability to restore the 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 it leverages from AWS, Azure, and GCP. Vercel's Services are designed to be fault tolerant.

4. Processes for regular testing, assessing and evaluating the effectiveness of technical and organizational 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, technical, and physical safeguards reasonably designed to protect the Services and Customer Data for 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 corporate and dedicated security team that manages Vercel's security program. Vercel's security program includes: (a) a security awareness program, (b) frequent security and privacy awareness training, (c) periodic internal and external assessments of the 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, Human Resources Security, Physical Security, Operations Security, Communications Security, Information Security Incident Management, Business Continuity & Crisis Management, Accountable Use and Code of Conduct, Supplier Management, Access Control, Cryptography, Secure Development, Vulnerability Management and security risk evaluation for all employees.

Security is managed at the highest levels of the company, with security and privacy reviews held regularly. Vercel maintains a dedicated security team to oversee 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 authorized access. Vercel personnel are granted access to Customer Data based on their assigned job duties and/or their position and authorized by senior management. Vercel personnel are authorized to access Customer Data based on their job function, role and responsibilities, and such access is subject to confidentiality and other contractual obligations. Employee access to Customer Data is revoked upon job 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 highly available service used for key storage and management. Customer modules to protect keys that cannot be retrieved from the service by anyone or any process outside of the region in which the key resides. Only Vercel SRE cryptographer and product team personnel for the Services run the technical controls are authorized.

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

Vercel is a remote first organization with no standard physical premises. Its network physical security controls for office spaces are inherited from our co-working providers' security programs. Vercel's Information Security Handbook covers physical security and remote office security.

The Services operate on AWS, Microsoft, and GCP and are protected by the security standards and controls of these third-party providers. Vercel's Information Security Handbook covers data center security.

Detailed information about Amazon's security is available at:

- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/fraud-detection-prevention/

For AWS EC2 Reports, please see:

- https://aws.amazon.com/compliance/ec2-faqs/

Detailed information about Microsoft's 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/security/infrastructure/

9. Measures for ensuring events logging.

Secure monitoring and logging is essential to timely and ensures the success or alerts Customer Data, including cloud services. Monitoring of security logs is centralized to Vercel's security team. Logs are tamper-proofed and reviewed as and when appropriate.

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

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

Vercel applies Secure Software Development Lifecycle Devices SDLC principles to the development of its Services. Vercel's Information Security Handbook covers the phases of the product cycle(s) lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, threat modeling, code review, static and dynamic analysis, and penetration testing. Vercel has not granted permission making to Customer Data.

Vercel adheres to a change management process to administer changes to the production environment for the Services, including, but not limited to, changes to software, applications, and systems. Patches are in place to modify the nature, frequency, and timeline of critical infrastructure and services that do not allow to be patched in a timely manner.

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, technical, and physical safeguards reasonably designed to protect the Services and Customer Data for 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 corporate and dedicated Information Security team that manages Vercel's security program. Vercel's security program includes: (a) a security awareness program, (b) frequent security and privacy awareness training, (c) periodic internal and external assessments of the 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, Human Resources Security, Physical Security, Operations Security, Communications Security, Information Security Incident Management, Business Continuity & Crisis Management, Accountable Use and Code of Conduct, Supplier Management, Access Control, Cryptography, Secure Development, Vulnerability Management and security risk evaluation for all employees.

Security is managed at the highest levels of the company, with security and privacy reviews held regularly. Vercel maintains a dedicated security team to oversee and coordinate company wide security initiatives.

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

Vercel conducts vendor third-party security to attest to various frameworks including SOC 2 Type 2 and continuous penetration testing.

AWS, Azure and GCP have ISO/IEC 27001, ISO 27017, and ISO 27018 certified, PCI DSS, SOC 1 and SOC 2 Security, Availability, and Confidentiality Reports, Vercel, Reasonable and Risk ICSA Certified, Trusted Cloud, FIPS 140-2, and Health Insurance Portability and Accountability Act (HIPAA) compliance standards for many other jurisdictions and industries. Frameworks. Further information about these providers' security practices can be found at the AWS Security website.

13. Measures for ensuring data minimization.

Vercel's Customers collect and process Customer Data. Vercel does not have access to Customer Data unless it is provided by Customer. Vercel's Services are designed to be a mission based, multi-tenant, hosted platform. Vercel provides tools within the Services that gives Customers the ability to delete Customer Data from the Services. Vercel's Information Security Handbook covers data minimization.

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

Vercel's Customers collect third-party security to attest to various frameworks including SOC 2 Type 2 and continuous penetration testing.

AWS, Azure and GCP have ISO/IEC 27001, ISO 27017, and ISO 27018 certified, PCI DSS, SOC 1 and SOC 2 Security, Availability, and Confidentiality Reports, Vercel, Reasonable and Risk ICSA Certified, Trusted Cloud, FIPS 140-2, and Health Insurance Portability and Accountability Act (HIPAA) compliance standards for many other jurisdictions and industries. Frameworks. Further information about these providers' security practices can be found at the AWS Security website.

15. Measures for ensuring data minimization.

Vercel's Customers collect and process Customer Data. Vercel does not have access to Customer Data unless it is provided by Customer. Vercel's Services are designed to be a mission based, multi-tenant, hosted platform. Vercel provides tools within the Services that gives Customers the ability to delete Customer Data from the Services. Vercel's Information Security Handbook covers data minimization.

Annex Customer's Orders and Supplier's Confirmations.

14. Measures for ensuring data quality.

Vernal has a Data Risk approach for ensuring data quality. These measures include: (a) not seeking to ensure the quality of data used to train SPI Labs, (b) ensuring that Vernal's Data Risk approach is reviewed by a data protection lawyer, (c) ensuring that the input values match expected values, Vernal applies these measures on the Customer Data prior to its use in the Vernal Services. Customer is responsible for ensuring that the Customer Data are accepting in accordance with the documentation.

Each Vernal Customer chooses what Customer Data they note through the Vernal Services and Vernal does not, and cannot, know what Customer Data are being uploaded. Responsibility rested. Vernal ensures that data quality is maintained from the time a Customer uploads Customer Data to the Vernal Services until that Customer Data leaves Vernal to the subsequent destination.

Vernal has a processes that allows individuals to exercise their privacy rights, as described in Vernal's Privacy Notice available at https://www.vernal.com/privacy-policy/.

15. Measures for ensuring limited data retention.

Vernal Customers unilaterally determine what Customer Data they note through the Vernal Services and Vernal does not, and cannot, know what Customer Data are being uploaded. Vernal responsibility rested. Customers have the ability to delete Customer Data via the self-service functionality of the Services. Vernal will, within a commercially reasonable period of time, delete Customer Data after the expiration or termination of Customer's Vernal Services, at Customer Sole Vernal's discretion, unless Vernal is required by law to retain such Customer Data.

16. Measures for ensuring accountability.

Vernal has adopted measures for ensuring accountability, such as implementing data protection policies across the business that are based on data minimization and Privacy Guidelines at https://www.vernal.com/), maintaining documentation on processing activities, and recording and reporting Security Incidents involving Personal Data, conducting Data Risk assessments, and implementing appropriate technical and organizational measures.

17. Measures for allowing data portability and ensuring erasure.

Vernal's Customers have direct relationships with their and users and are responsible for responding to requests from Data Subjects and users wish to exercise their rights under Applicable Data Protection Laws.

Vernal has self-service functionality that allows Customers to delete and suppress their Customer Data.

Vernal specifies in the Agreement that it will provide assistance to such Customer as reasonably required by such Customer to enable such Customer to comply with Applicable Data Protection Laws in respect to requests from individuals to exercise their rights under Applicable Data Protection Laws (e.g. rights of data access, rectification, erasure, restriction, objection, and portability, as applicable) (collectively, "DSR"). Vernal is subject to orders from Customer Data, Vernal will advise that Data Subject to contact the Customer in accordance with Customer's instructions and Customer will be responsible for responding to any such request.

Vernal has a process that allows individuals to exercise their privacy rights as described in Vernal's Privacy Notice available at https://www.vernal.com/privacy-policy/.

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

When Vernal engages a Subprocessor under this Addendum, Vernal and the Subprocessor shall enter into an agreement with substantially similar terms to those contained herein. Such Subprocessor agreement must ensure that Vernal is able to meet its obligations to Customer. In addition to implementing technical and organizational measures, Vernal and its Subprocessors must assist by all a) notify Vernal in the event of a Security Incident or Vernal may notify Customers of a Security Incident, b) assist Customers in the event of a Customer's DPIA or PIA, and c) provide Customers with information and assistance as Customer and Vernal agree in writing or as may be required to fulfill Customer's obligation under GDPR to respond to requests for exercising of Data Subject rights.

Vernal has a process that allows individuals to exercise their privacy rights as described in Vernal's Privacy Notice available at https://www.vernal.com/privacy-policy/.

Schedule 3: Cross Border Data Transfer Mechanism

1. Definitions:

1. "**Standard Contractual Clauses**" means the Standard Contractual Clauses attached hereto pursuant to EC Decision 2010/87/EU;
2. "**UK GDR**" means the UK International data transfer addendum (Schedule 5).

2. UK GDPA

For data transfers from the United Kingdom, the UK GDPA will be deemed entered into (and incorporated into this Addendum) by reference together with the Standard Contractual Clauses, as varied by the UK GDPA.

3. The 2021 Standard Contractual Clauses

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

1. **Module One Controller to Controller** will apply where Customer is a controller of Service Generated Data and/or Contact Data and Vernal is a controller of Service Generated Data and/or Contact Data under Applicable Data Protection Laws;
2. **Module Two Controller to Processor** will apply where Customer is a controller of Customer Data and Vernal is a processor of Customer Data;
3. **Module Three Processor to Processor** will apply where Customer is a processor of Customer Data and Vernal is a processor of Customer Data;
4. For each module, where applicable:
   - In Clause 7 the optional docking clause will not apply;
   - In Clause 9(a) Option 2 (General Written Authorisation) shall apply and the time period of Subprocessor changes will be as set forth in Section 7 (Subprocessors) of this Addendum;
   - In Clause 11, the optional language will not apply;
   - In Clause 17 Option 1, the SCC Governing Standard Contractual Clauses will be the laws of Ireland;
   - In Clause 18(b) disputes will be resolved before the courts of Ireland;
   - In Annex I Part A:
     Data Exporter: Customer and authorized Affiliates of Customer;
     Contact details: Customer's address and contact details provided to Vernal;
     Data Exporter Role: The Data Exporter's role is as set forth in Section 2 of this Addendum;
     Signature & Date: By entering into this 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: Vernal;
     Contact Details: Vernal Privacy - privacy@vernal.com
     Data Importer Role: The Data Importer's role is outlined in Section 2 of this Addendum;
     Signature & Date: By entering into this 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.
   - In Annex I Part B: The categories of data subjects are described in Schedule 1 Section 2;
   - The frequency of the transfer is anticipated to be described in Schedule 1 Section 3. 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 7;
   - The subprocessor transfers are as described in Schedule 1 Section 8 and duration of the processing is outlined at https://www.vernal.com/;
   - In Annex I Part C: The Irish Data Protection Commission will be the competent supervisory authority;
   - Schedule 2 serves as Annex II of the Standard Contractual Clauses.
4. As to the specific modules, the parties agree that the following modules apply, as applicable, in accordance with Section 2:
   - Controller-Controller - Module One
   - Controller-Processor - Module Two
   - Processor-Processor - Module Three
5. To the extent there is any conflict between the Standard Contractual Clauses or UK GDPA and any other terms in this Addendum, the Agreement, or the Customer Subscribe Specific Terms the provisions of the Standard Contractual Clauses or the UK GDPA, as applicable, will prevail.

Schedule 4: Jurisdiction Specific Terms

1. California

1. The definition of "**Applicable Data Protection Laws**" includes the California Consumer Privacy Act ("**CCPA**");
2. The terms "**business**", "**commercial purpose**", "**service provider**", "**sell**", "**share**" and "**personal information**" shall have the meanings set forth in the CCPA;
3. To the extent Vernal processes personal information as a Processor under Section A.4 of the Addendum:
   1. Vernal shall not sell Customer Data;
   2. Vernal will not share or retain Customer Data for cross-context behavioral advertising;
   3. Vernal will not retain, use or disclose Customer Data (i) except as necessary for the business purpose of providing the Services, including retaining, using or disclosing the Customer Data for a commercial purpose other than providing the Services, or (ii) outside of the direct business relationship between Vernal and Customer;
   4. The parties acknowledge and agree that the Processing of Customer Data authorized by Customer's instructions described in Section A.2 of this Addendum is integral to and incorporated by Vernal's provision of the Services and the direct business relationship between the parties;
   5. Notwithstanding anything in the Agreement or any Order Form entered or hereafter entered between Customer and Vernal, Vernal's access to Customer Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement;
4. To the extent Vernal processes personal information as a Controller under Section A.5 of the Addendum:
   1. Vernal is the business under the CCPA with respect to such data;
   2. Vernal will process such data for the purposes described in the Agreement, or as otherwise permitted by the CCPA;
   3. Vernal will be responsible for compliance notices of the CCPA, including providing the special notice of sale prohibited required of businesses under the CCPA, and responding to consumer requests to exercise their CCPA rights;
   4. Vernal, in its capacity as a business, Vernal and sales representatives and appropriate steps to make available to Customer information its demonstrate, in relation to such data, Vernal's compliance with applicable provisions of the CCPA, including, by way of illustration, contracts, records of consumer requests made between Vernal or using such data or uncontrolled personal, Vernal and sales representatives and appropriate steps to work with Customer to remediate improper use of such data by Vernal; and
   5. Vernal implements and maintains reasonable security and privacy procedures appropriate to the nature of the personal information that it processes as set forth in section A of this Addendum.

2. EEA

1. The definition of "**Applicable Data Protection Laws**" includes the General Data Protection Regulation (EU) 2016/679 ("**GDPR**");
2. When Vernal engages a Subprocessor under Section 7.1(Subprocessors) it will:
   1. require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the terms set out in Article 32(1) and (4) of the GDPR and in clauses 7.2 to 7.4 of this addendum, and ensure such Subprocessor is subject to appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and
   2. 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; and
   3. **GDPR Penalties.** Notwithstanding anything to the contrary in this Addendum or other agreement, Customer shall indemnify and keep indemnified and defend at its own expense Vernal against all costs, claims, damages or expenses incurred by Vernal or for which Vernal may become liable due to any failure by Customer or its employees or agents to comply with the obligations under this section.
3. Vernal implements and maintains reasonable security and privacy procedures appropriate to the nature of the personal information that it processes as set forth in section A of this Addendum.

3. United Kingdom

1. The definition of "**Applicable Data Protection Laws**" includes the Data Protection Act 2018 ("**DPA 2018**");
2. When Vernal engages a Subprocessor under Section 7.1(Subprocessors) it will:
   1. require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the terms set out in Article 32(1) and (4) of the GDPR and in clauses 7.2 to 7.4 of this addendum, and ensure such Subprocessor is subject to appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and
   2. require any appointed Subprocessor to agree in writing only to 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; and
   3. **GDPR Penalties.** Notwithstanding anything to the contrary in this Addendum or other agreement, Customer shall indemnify and keep indemnified and defend at its own expense Vernal against all costs, claims, damages or expenses incurred by Vernal or for which Vernal may become liable due to any failure by Customer or its employees or agents to comply with the obligations under this section.
3. Vernal implements and maintains reasonable security and privacy procedures appropriate to the nature of the personal information that it processes as set forth in section A of this Addendum.

4. Switzerland

1. The definition of "**Applicable Data Protection Laws**" includes the Swiss Federal Data Protection Act ("**FDPA**");
2. When Vernal engages a Subprocessor under Section 7.1(Subprocessors) it will:
   1. require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the terms set out in Article 32(1) and (4) of the GDPR and in clauses 7.2 to 7.4 of this addendum, and ensure such Subprocessor is subject to appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and
   2. require any appointed Subprocessor to agree in writing only to 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; and
3. Vernal implements and maintains reasonable security and privacy procedures appropriate to the nature of the personal information that it processes as set forth in section A of this Addendum.

5. Canada

1. As the definition of "**Applicable Data Protection Laws**" includes the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), the parties agree that:
   1. Vernal's Subprocessors, as described in this Addendum, are third parties under the PIPEDA, with whom Vernal has entered into a written contract that includes terms substantially similar to this Addendum. Vernal has conducted appropriate due diligence on its Subprocessors;
   2. Vernal will implement technical and organizational measures as set forth in Section 7.2.

Schedule 5: UK DTA

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

Part 1: Tables

Table 1: Parties

Start date	As Effective Date of the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
	Full legal name: Vernal Inc.	Trading name (if different): n/a
Parties' details	Data Exporter	Data Importer
	Main address (if a company registered address): 1 Sansome St, Ste 3500, San Francisco, CA 94104	Official registration number (if any) (company number or similar identifier): Delaware 5800244
Key Contact	Data Exporter	Contact details including email: privacy@vernal.com
Signature (if required for the purposes of Section 2)	By entering into the Agreement, Data Exporter is deemed to have signed this Addendum as of the Effective Date of the Agreement.	By entering into the Agreement, Data Importer is deemed to have signed this Addendum as of the Effective Date of the Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The approved EU SCCs including the Appendix Information and 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 Annexes
Annex II:	Technical and organizational measures including technical and organizational measures to ensure the security of the data: See Annexes
Annex III:	List of Sub-processors (Modules 2 and 3 only): See Schedule 3 Section 7.1(Subprocessors)

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 purposes of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally bound by the Addendum and place data subjects in a position that rights set out in the Addendum apply to their Personal Data. This Addendum shall not apply to the extent that the parties enter into an agreement the Approved EU SCCs and any part of the Addendum is varied or replaced.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs 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 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 subject rights, which is deemed by UK Data Protection Laws when you are making a Restricted Transfer to be adequate to enable the processing of the relevant Personal Data.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the UK 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 United Kingdom, including 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 its Clause 3 (Utility Not Prohibit obligations) to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendments(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take place instead.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If a clause ending 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 beforehand thought or discussion relating to this Addendum or its clauses or any provision of it will not mean that it is to be interpreted against the parties who drafted it. Also, any ambiguity will be resolved in favor of a meaning that clarifies that legislation for specific protection has been consideration, or enacted and/or amended from time to time, unless that meaning is not possible.

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 this Addendum, the following order of precedence applies:
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 to the extent) the inconsistent or conflicting provision of the Addendum EU SCCs provides greater rights or benefits 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. they operate for transfers made by the data exporter 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. Section 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 governed by the laws of England and Wales and any dispute arising from it is resolved by the courts of England and Wales or, if each case unless the law of a country or territory or state 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 14 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 purposes 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 46(2) of Regulation (EU) 2016/679";
    c. Clause 6 (Description of the transfer(s)) is replaced with:
    "The details of the transfer(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 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) 2018/1725" "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 "Regulation (EU) 2016/679" are replaced with "UK Data Protection Laws". References to "Member State" and "EU Member State" are replaced with "United Kingdom";
    g. References to Regulation (EU) 2018/1725 are removed;
    h. References to the "Union", "EU" and "EU Member State" are replaced with "United Kingdom";
    i. The reference to Clause 12(1) of Clause 10(b) of Module one, is replaced with "Clause 10(b)";
    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 law(s) of England and Wales (not Member State) in 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.".
16. The Mandatory Clauses of the Approved EU SCCs are that form part of the Addendum, except for Sections 9, 10 and 11.

Amendments to this Addendum

17. The Parties may agree to change Clause 17 and/or 18 of the Addendum EU SCCs to enable it to operate as a transfer tool under UK Data Protection Laws.
18. 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 changes in writing, provided that the changes do not reduce the Appropriate Safeguards.
19. They may from time to time elect to vary certain parts of this Addendum:
    a. notice reasonable and proportionate changes to the Approved Addendum, including concluding amend a the Approved Addendum, which:
    b. reflects changes to UK Data Protection Laws. The revised Approved Addendum specifies the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appropriate Information. This Addendum is then deemed amended, and the Parties must act in accordance with it from the start date specified.
20. If the EU Commission is revised Approved Addendum Under Section 19 in any Time the Parties, and if part of the Addendum to which the amendments changed, will an a direct result of the changes to the Approved Addendum has a substantial, disproportionate and demonstrable increase:
    a. its direct cost 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 to a reasonable level, then the Parties shall co-operate in good faith to amend 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.
21. The Parties do not intend the amendment of this Addendum to detract from this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.