Netlify Data Processing Agreement

Last Updated: November 1st, 2023

This Data Processing Agreement ("**DPA**") forms part of the Enterprise Master Subscription Agreement and the Self-Serve Subscription Agreement, as applicable, unless Customer has entered into a superseding written agreement with Netlify, in which case, it forms part of such written agreement (in either case, the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term "**Customer**", shall include Customer and its Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services under the Agreement, Netlify may Process certain Customer Data (such terms defined below) on behalf of Customer and where Netlify Processes such Customer Data on behalf of Customer the Parties agree to comply with the terms and conditions in this DPA in connection with the processing of such Customer Data, each acting reasonably and in good faith.

1 Definitions

1.1 "**Applicable Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Customer Data under the Agreement as amended from time to time.

1.2 "**Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Netlify.

1.3 **"CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations, as amended by the California Privacy Rights Act of 2020, and any other legislative and/or regulatory amendments or successors thereto.

1.4 **"Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.5 **"Customer"** means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates).

1.6 "**Customer Data**" means Personal Data that is described in Exhibit 1 and any other Personal Data that is Processed by Netlify pursuant to the Agreement and this DPA;

1.7 **"Data Subjec**t" means the identified or identifiable natural person to whom Personal Data relates.

1.8 **"GDPR"** means 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, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the UK.

1.9 "**Netlify Group**" means Netlify and any companies under the direct or indirect control of Netlify, Inc who are engaged in the Processing of Customer Data.

1.10 "**Personal Data**" means any information relating to: (i) an identified or identifiable natural person, and(ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under Applicable Data Protection Laws).

1.11 "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Netlify or its Sub-processors of which Netlify becomes aware.

1.12 "**Processing**" or "**Process**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

1.13 "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

1.14 "**Public Authority**" means any government agency or law enforcement authority.

1.15 "**Restricted Transfer**" means: (i) a transfer of Personal Data from a Controller to a Processor; or (ii) an onward transfer of Personal Data from a Processor to a Sub-processor, in each case, where such transfer would be prohibited by Applicable Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Data Protection Laws) in the absence of the EU Standard Contractual Clauses or the IDTA.

1.16 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Netlify for Customer pursuant to the Agreement.

1.17 "**EU Standard Contractual Clauses**" means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

1.18 "**IDTA**" means the UK international data transfer addendum to the EU Commission standard contractual clauses issued by the Information Commissioner's Office laid before Parliament in accordance with s119A of the UK Data Protection Act 2018 and effective on 21 March 2022.

1.19 "**Sub-processor(s)**" means any Processor engaged by Netlify or a member of the Netlify Group to Process Customer Data.

1.20 "**Supervisory Authority**" means a government agency or law enforcement authority, including judicial authorities responsible for the enforcement of Applicable Data Protection Laws.

1.21 "**UK**" means the United Kingdom.

2 Data Processing Terms

2.1 This DPA applies where Netlify Processes Customer Data as a Processor on behalf of Customer and such Customer Data is subject to Applicable Data Protection Laws. Provisions applicable to Netlify as Processor shall apply also when Netlify Processes Customer Data on behalf of Customer as sub-processor.

2.2 The parties have agreed to enter into this DPA in order to ensure that appropriate safeguards are in place to protect Customer Data in accordance with Applicable Data Protection Laws. Accordingly, Netlify agrees to comply with the provisions of this DPA in respect of any Customer Data .

2.3 Each party warrants that it will comply with Applicable Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality and legality of Customer Data and the means by which the Customer acquired Customer Data.

2.4 If Customer is a Processor, Customer warrants to Netlify that Customer's instructions and actions with respect to Customer Data, including its appointment of Netlify as sub-Processor and, where applicable, concluding the EU Standard Contractual Clauses, have been (and will, for the duration of this DPA, continue to be) authorized by the relevant third-party Controller.

Customer shall be solely responsible for forwarding any notifications received from Netlify to the relevant Controller where appropriate.

3 Ownership of Customer Data

3.1 All Customer Data processed by Netlify as a Processor on behalf of Customer under the terms of this DPA shall remain the property of Customer. Under no circumstances, will Netlify act, or be deemed to act, as a Controller of Customer Data under any Applicable Data Protection Laws.

3.2 The parties agree that the type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Exhibit 1.

4 Netlify Obligations

4.1 With respect to the Customer Data Netlify Processes in its role as Processor under this DPA Netlify shall:

(a) only Process the Customer Data in order to provide the Services and in accordance with Customer's written instructions as set out in the Agreement and this DPA, unless required to do so by Applicable Data Protection Laws. If Netlify is required to Process Customer Data under Applicable Data Protection Laws, Netlify shall inform the Customer of such a legal requirement before Processing, unless that law prohibits the provision of such information;

(b) not sell, retain, use or disclose the Customer Data for any purpose (whether or not commercial) other than for the specific purpose of performing the Services. Netlify shall not use the Customer Data for the purposes of marketing or advertising. Netlify's performance of the Services may include disclosing Customer Data to Sub-processors where this is in accordance with section 6 of this DPA;

(c) inform Customer if, in Netlify's opinion, any instructions provided by Customer under section 4.1(a) infringe Applicable Data Protection Laws;

(d) ensure that only authorized personnel have access to such Customer Data and that such personal whom it authorizes to have access to the Customer Data are under contractual or statutory obligations of confidentiality.

5 Rights of Data Subjects

5.1 Netlify shall reasonably cooperate with Customer in case of any complaint, dispute or request it has received from a Data Subject under Applicable Data Protection Laws such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Netlify shall not respond to a Data Subject Request itself, except that Customer authorizes Netlify to redirect the Data Subject Request as necessary to allow Customer to respond directly. Netlify shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Netlify is legally obliged or permitted to do so.

6 Sub-Processors

6.1 Authorization for Onward Sub-processing. Customer hereby provides a general authorisation for Netlify to engage onward Sub-Processors provided that:

(a) Netlify will restrict the onward Sub-processor's access to Customer Data only to what is strictly necessary to provide the Services and in accordance with the Agreement;

(b) Netlify agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect Customer Data, on any Sub-processor it appoints that requires such Sub-processor to protect Customer Data to the standard required by Applicable Data Protection Laws being no less than the obligations to which Netlify is subject under this DPA;

(c) Netlify shall remain liable for any breach of this DPA that is caused by any act, error, or omission of its Sub-processors.

6.2 List of Current Sub-Processors and Notification of New Sub-Processors. The current list of Sub-Processors engaged in Processing Customer Data for the performance of the Services, including a description of their processing activities and countries of location is located at https://www.netlify.com/legal/subprocessors/. Customer hereby confirms its general written authorisation in accordance with Article 28 GDPR, to these Sub-processors, their locations and Processing activities as it pertains to Customer Data. Netlify shall provide notification to the Customer of the appointment of a new Sub-processor before authorizing any new Sub-processor to Process Customer Data in connection with the provision of the applicable Services by updating the above link.

6.3 Objection Right for New Sub-Processors. Customer may object to Netlify's use of a new Sub-processor by notifying Netlify in writing within thirty (30) days of receipt of Netlify's notice in accordance with the mechanism set out in section 6.2 above, provided such objection is in writing and based on reasonable grounds relating to data protection. Upon receipt of an objection from the Customer to the use of a new Sub-processor, Netlify will use reasonable efforts to make available to Customer a change in the Service(s) to avoid processing of Customer Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Netlify is unable to make available such change, Customer may terminate the applicable Order Forms with respect only to those Services which cannot be provided by Netlify without the use of the objected-to new Sub-processor by providing written notice to Netlify. Netlify will refund Customer any prepaid fees covering the remainder of the term of such Order Forms following the effective date of such termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

7 Security

7.1 Security Measures. Netlify shall implement and maintain appropriate technical and organizational measures for protection of the security of the Customer Data, including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in Exhibit II, and in particular, where reasonably deemed necessary by the Customer through the use of: (i) the pseudonymisation and/or encryption of Customer Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Customer Data in the event of a physical or technical incident; and/or (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. Netlify regularly monitors compliance with these measures. Netlify will not materially decrease the overall security of the Services during the term of the Agreement.

8 Audit.

8.1 The parties acknowledge that Customer must be able to assess Netlify's compliance with its obligations under Applicable Data Protection Laws and this DPA, insofar as Netlify is acting as a Processor on behalf of Customer. Netlify shall maintain an audit program to help ensure compliance with the obligations set forth in this DPA and shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA as set forth in this section 8.

8.2 Netlify uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Data. Such audits are performed at least once annually at Netlify's expense by independent third-party security professionals chosen by Netlify which results in the generation of a confidential audit report ("**Audit Report**").

8.3 Upon Customer's written request, at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Netlify shall make available to the Customer a copy of Netlify's most recent Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Laws will not extend beyond the provision of these Audit Reports.

8.4 On-Site Audit. Customer may request to access Netlify's premises to audit Netlify's Processing activities covered by this DPA ("**On-Site Audit**") only when:

(a) the Audit Report does not provide sufficient information to demonstrate compliance with this DPA;

(b) Customer has received a notice from Netlify of a Personal Data Breach;

(c) Such an audit is required by Application Data Protection Laws or by a Customer's competent Supervisory Authority.

8.4.1 Any On-Site Audit will be limited to Customer Data Processing and storage facilities operated by Netlify or any of Netlify's Affiliates. Customer acknowledges that Netlify operates a multi-tenant cloud environment. Accordingly, Netlify shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Netlify customers' information.

8.4.2 Any On-Site Audit shall be conducted by Customer or its third-party auditor acting reasonably, in good faith, and in a proportionate manner, taking into account the nature and complexity of the Services used by the Customer, on a maximum of one occasion every 12 months and by providing at least four weeks' advance write notice to security@netlify.com and legal@netlify.com. Before any On-Site Audit commences, Customer and Netlify shall mutually agree upon the scope, timing and duration of the audit and reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Netlify. Customer must promptly provide Netlify with information regarding any non-compliance discovered during the course of an On-Site Audit.

8.4.3 The parties agree that Customer's right to access Netlify's premises under the EU Standard Contractual Clauses shall be exercised according to this section 8.

9 Data Protection Impact Assessment.

9.1 Upon Customer's request, Netlify shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Applicable Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Netlify.

10 Security Incident Notification Management and Notification

10.1 Netlify maintains security incident management policies and procedures specified in Exhibit II and shall notify Customer without undue delay, but in any event within forty-eight (48) hours, in the event of a confirmed Personal Data Breach affecting Customer Data and to take appropriate measures to mitigate its possible adverse effects.

10.2 Netlify shall make reasonable efforts to identify the cause of such Personal Data Breach and take such steps as Netlify deems necessary and reasonable to remediate the cause of such the Personal Data Breach to the extent the remediation is within Netlify's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users.

11 Public Authority Access Requests

11.1 If Netlify becomes aware of a Public Authority requesting Customer Data that Netlify processes on behalf of Customer in its role as Processor then Netlify will:

(a) immediately notify Customer of the request unless such notification is legally prohibited;

(b) inform the Public Authority that it is a Processor of the Customer Data and is not authorized to disclose the Customer Data without Customer's consent;

(c) disclose to Public Authority the minimum necessary Customer contact details to allow the Public Authority to contact the Customer and instruct the Public Authority to direct its data request to Customer;

(d) to the extent that Netlify reviews the request with reasonable efforts and as a result is able to identify that such Public Authority process requesting Customer Data raises a conflict of law, pursue legal remedies prior to producing Customer Data up to an appellate court level; and

(e) to the extent Netlify provides access to or discloses Customer Data in response to a Public Authority legal process either with Customer authorization or due to a mandatory legal compulsion, then Netlify will disclose the minimum amount of Customer Data to the extent it is legally required to do so and in accordance with the applicable legal process.

11.2 Section 11.1(b) above shall not apply in the event that Netlify has a good-faith belief the Public Authority request is necessary due to an emergency involving the danger of death or serious physical injury to an individual.

11.3 As of the date Customer entered into this DPA with Netlify, Netlify makes the commitments listed below:

(a) Netlify has never turned over our encryption or authentication keys or its customers' encryption or authentication keys to any Public Authority;

(b) Netlify has never installed any law enforcement software or equipment anywhere on its network;

(c) Netlify has never provided any law enforcement organization a feed of its customers' content transiting our network; and

(d) Netlify has never weakened, compromised, or subverted any of its encryption at the request of law enforcement or another third party.

12 Return and Deletion of Customer Data

12.1 Upon termination of Customer’s access to and use of the Services, Netlify shall either: (a) at Customer’s request, permit Customer to export its Customer Data, at its expense; or (b) delete all Customer Data in accordance with the capabilities of the Service and, where applicable, Article 28 (3) (g) of the GDPR. Following such period, Netlify shall delete all Customer Data stored or processed by Netlify on behalf of Customer in accordance with Netlify’s deletion policies and procedures. Customer expressly consents to such deletion.

13 Limitation of Liability

13.1 This DPA shall be subject to the limitations of liability set forth in the Agreement. For the avoidance of doubt, Customer acknowledges and agrees that Netlify’s total liability for all claims from Customer or its Affiliates arising out of or relating to the Agreement and this DPA shall be considered in aggregate for all claims under both the Agreement and this DPA. This section shall not be construed as limiting the liability of either party with respect to claims brought by data subjects.

14 Data transfers from the EEA, Switzerland, and the UK

14.1 In connection with the Services, the parties anticipate that Netlify (and its Sub-processors) may Process outside of the European Economic Area ("**EEA**"), Switzerland, and the United Kingdom, certain Customer Data protected by Applicable Data Protection Laws in respect of which Customer may be a Controller. In such circumstances, Netlify will be the data importer and Customer the data exporter.

14.2 Netlify has certified to participate in and comply with the EU-U.S. DPF, and the UK Extension to the EU-U.S. DPF (see: https://www.dataprivacyframework.gov/s). The parties agree that when the transfer of Customer Data protected by the GDPR or UK GDPR from Customer to Netlify is a Restricted Transfer such transfer shall take place on the basis of the EU-US Data Privacy Framework ("**EU-US DPF**"), or the UK Extension to the EU-US DPF, as applicable. In the event the Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to the EU-US DPF or the UK Extension to the EU-US DPF. If the EU-US DPF or the UK Extension to the EU-US DPF is declared invalid, or if Netlify fails to re-certify for the EU-US DPF, then the transfer of Personal Data will be subject to the provisions below.

14.3 The parties agree that when the transfer of Customer Data protected by the GDPR from Customer to Netlify is a Restricted Transfer, and is not subject to the EU-US DPF, or the UK Extension to the EU-US DPF, then it shall be subject to the EU Standard Contractual Clauses in accordance with the following provisions.

14.3.1 Module Two will apply where Customer is a Controller and Module Three will apply where Customer is a Processor.

14.3.2 In Clause 7, the optional docking clause will apply.

14.3.3 The parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 and 16(d) of the EU Standard Contractual Clauses shall be provided by Netlify to Customer only upon Customer's written request.

14.3.4 The parties agree that the audits described in Clause 8.9 of the EU Standard Contractual Clauses shall be carried out in accordance with section 8 of this DPA.

14.3.5 In Clause 9, Option 2 will apply. Netlify has Customer's general authorisation to engage Sub-processors in accordance with section 6 of this DPA, and the time period for prior notice of sub-Processor changes shall be as set out in section 6.2 of this DPA.

14.3.6 In Clause 11, the optional language will not apply;

14.3.7 Clause 13 shall apply as follows:

(a) Where Customer is established in an EU Member State, the Supervisory Authority with responsibility for ensuring compliance by Customer with GDPR as regards the data transfer shall act as competent Supervisory Authority.

(b) Where Customer is not established in an EU Member State but falls within the territorial scope of application of GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1), the Supervisory Authority of the Member State in which the representative within the meaning of Article 27(1) of GDPR is established shall act as competent Supervisory Authority.

(c) Where Customer is not established in an EU Member State, but falls within the territorial scope of application of GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2), the Data Protection Commission - 21 Fitzwilliam Square South, D02RD28 Dublin, Ireland shall act as competent Supervisory Authority;

(d) Where Customer is established in the United Kingdom or falls within the territorial scope of application of the UK GDPR, the Information Commissioner's Office (“**ICO**”) shall act as competent Supervisory Authority.

14.3.8 Clause 15(1)(a) shall apply as detailed in section 11 of this DPA, and Netlify shall notify Customer (only) and not the Data Subject(s) in case of Public Authority access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

14.3.9 In Clause 17, Option 1 will apply, and the EU Standard Contractual Clauses will be governed by the laws of Ireland.

14.3.10 In Clause 18(b), disputes shall be resolved before the courts of Ireland.

14.3.11 Annex I of the EU Standard Contractual Clauses shall be deemed completed with the information set out in Exhibit I to this DPA.

14.3.12 Annex II of the EU Standard Contractual Clauses shall be deemed completed with the information set out in Exhibit II to this DPA.

14.4 The parties agree that when the transfer of Customer Data is protected by the UK GDPR and is not subject to the UK Extension to the EU-US DPF, the IDTA will apply in accordance with the following provisions.

14.4.1 The EU Standard Contractual Clauses, completed as set out above in section 14.3 of this DPA, shall also apply to transfers of such Customer Data, subject to section 14.4.2 below.

14.4.2 The IDTA shall be deemed executed between the transferring Customer and Netlify, and the EU Standard Contractual Clauses shall be deemed amended as specified by the IDTA in respect of the transfer of such Customer Data and the IDTA mandatory clauses shall apply. The information required for Tables 1 to 3 of Part One of the IDTA is set out in Exhibits I to II of this DPA (as applicable). For the purposes of Table 4 of Part One of the IDTA, neither party may end the IDTA when it changes.

14.4.3 The IDTA shall be subject to the laws of England and Wales, and subject to the jurisdiction of the courts of England and Wales.

14.5 The parties agree that when the transfer of Customer Data is protected by the Swiss Federal Act on Data Protection (as amended or replaced), the EU Standard Contractual Clauses, completed as set out about in section 14.3 of this DPA, shall apply to transfers of such Customer Data, except that:

(a) the competent Supervisory Authority in respect of such Customer Data shall be the Swiss Federal Data Protection and Information Commissioner;

(b) in Clause 17, the governing law shall be the laws of Switzerland;

(c) references to "Member State(s)" in the EU Standard Contractual Clauses shall be interpreted to refer to Switzerland, and data subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU Standard Contractual Clauses in Switzerland; and

(d) references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the Standard Contractual Clauses shall be understood to be references to the Swiss Federal Act on Data Protection (as amended or replaced).

14.6 In respect of Restricted Transfers made to Netlify under section 14.3 of this DPA, Netlify shall not participate in (nor permit any Sub-processor to participate in) any further Restricted Transfers of Customer Data (whether as an "exporter" or an "importer" of the Customer Data) unless such further Restricted Transfer is made in full compliance with Applicable Data Protection Laws and pursuant to the EU Standard Contractual Clauses and the IDTA, as applicable, being implemented between the exporter and importer of the Customer Data.

15 Governing Law and Jurisdiction

15.1 This DPA is governed by the laws of Ireland, and is subject to the exclusive jurisdiction of the courts of Ireland. Notices under this DPA shall be sent in accordance with the notice provisions of the Agreement.

EXHIBIT I

Details of Processing

1. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

Name: Customer and its Affiliates, as identified in the Agreement

Address: as listed in the Agreement

Contact person's name, position and contact details: as listed in the Agreement

Activities relevant to the data transferred under these clauses: Use of the Services pursuant to the Agreement and as further described in the Order Form and the online documentation.

Role: For the purposes of Module Two of the EU Standard Contractual Clauses, Customer and/or its Affiliate is a Controller. For the purposes of Module Three of the EU Standard Contractual Clauses Customer and/or its Affiliate is a Processor.

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

Name: Netlify, Inc.

Address: 512 2nd Street, Suite 200, San Francisco, CA 94107

Contact person's name, position and contact details: privacy@netlify.com

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement, as further described in the Agreement, the applicable Order Form, and online documentation.

2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);

- Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);
- Employees, agents, advisors, and freelancers of the data exporter (who are natural persons);
- Customers' own website visitors, where the website is hosted by Netlify; and/or
- Customer's Users authorized by Customer to use the Services

3. CATEGORIES OF PERSONAL DATA TRANSFERRED

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Localization data
- IP address

4. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)

- None

5. FREQUENCY OF THE TRANSFERS

Continuous basis depending on the use of the Services by Customer.

6. NATURE OF THE PROCESSING

The nature of the Processing is the performance of the Services pursuant to the Agreement.

7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

Netlify will Process Customer Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Agreement, the Order Form and online documentation, and as further instructed by Customer in its use of the Services.

8. DURATION OF PROCESSING

Subject to section 12 of this DPA, Netlify will Process Customer Data for the duration of the Agreement, unless otherwise agreed upon in writing.

EXHIBIT II

Netlify Technical and Organizational Security Measures - Enterprise Services

Netlify has implemented and maintains an information security program in accordance with SOC2 Type II and ISO 27001 standards. Netlify reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections set forth in this document.

1. Information Security Program and Team:

The Netlify security program includes documented policies and standards of administrative, technical, physical and organisational safeguards, which govern the handling of Customer Data in compliance with Applicable Data Protection Laws. The security program is designed to protect the confidentiality and integrity of Customer Data appropriate to the nature, scope, context and purposes and the risks involved in the Processing of the Personal Data for individuals. Netlify maintains a security team which is on call 24/7 to respond to security alerts and events.

1. SECURITY ORGANIZATION. Netlify has designated a Chief Information Security Officer or equivalent responsible for coordinating, managing, and monitoring Netlify's information security function, policies, and procedures.
2. POLICIES. Netlify's information security policies are (i) documented; (ii) reviewed and approved by executive management, including after material changes to the Services; and (iii) published, and communicated to personnel, contractors, and third parties with access to Personal Data, including appropriate ramifications for non-compliance.
3. RISK MANAGEMENT. Netlify performs information security risk assessments as part of a risk governance program that are established with the objective to regularly test, assess and evaluate the effectiveness of the Security Program. This assessment is designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry standard practices, and changing security threats. Netlify has our risk program audited annually by an independent third-party in accordance with applicable controls.
4. CURRENCY. Netlify updates the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will reduce the commitments, protections, or overall level of service provided to Customers as described herein.

2. Security Certifications

Netlify has established and maintains sufficient controls to meet certification and attestation for the objectives stated in ISO 27001 and SOC 2 Type II. At least once per calendar year, Netlify will produce an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Customer.

3. Measures of Encryption of Personal Data

Netlify uses NIST approved encryption algorithms no less than 128-bit encryption to encrypt Personal Data in transit over public networks to the Services or at rest on Netlify controlled systems.

4. System and Data Access Controls to maintain Confidentiality of Personal Data

These controls vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documentation authorisation processes, documented change management processes and/or logging of access on several levels.

Access to the Services by Netlify employees and contractors are protected by authentication and authorization mechanisms in accordance with NIST 800-63B (Authentication and Lifecycle Management) or equivalent standard. Authentication is required to gain access to any system within the Services. Individuals are assigned a unique user account. Individual user accounts are not shared. Access privileges are based on job requirements using the principle of least privilege access and are revoked within 24 hours upon termination of employment or consulting relationships. Access entitlements are reviewed by management quarterly. Infrastructure access includes appropriate user account and authentication controls, which include the required encrypted two-factor authenticated connections.

5. Measures to ensure Personal Data protected from accidental loss or destruction by maintaining:

A. LOGGING AND MONITORING. Netlify has logging enabled for all components that support the Services, and (1) are centrally collected; (2) are secured in an effort to prevent tampering; (3) are monitored for anomalies by a trained security team; and (4) retained on-line for 90 days and offline for 1 year.

B. FIREWALL SYSTEM. Netlify uses an industry-standard firewall technologies to protect Netlify systems and it inspects all ingress connections and all egress connections. Cloud monitoring tools are enabled to alert on improper configurations and weaknesses.

C. VULNERABILITY MANAGEMENT. Netlify conducts security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide remediation. When software vulnerabilities are revealed and addressed by a vendor patch, Netlify obtains the patch from the applicable vendor and applies it within an appropriate time frame in accordance with Netlify's vulnerability management and security patch management standard operating procedures and only after such patch is tested and determined to be safe for installation in all production systems.

D. ANTIVIRUS. Netlify endpoint antivirus software is updated at regular intervals as determined by the vendor.

E. CHANGE CONTROL. Netlify evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following Netlify's standard operating procedure.

F. DATA SEPARATION. Customer Data is logically separate from Netlify's other customers and Netlify's corporate infrastructure.

G. CONFIGURATION MANAGEMENT. Netlify has implemented and maintains standard hardened configurations for all system components within the Service. Netlify uses industry standard hardening guides when developing standard hardening configurations.

H. SECURE SOFTWARE DEVELOPMENT. Netlify has implemented and maintains secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten. All personnel responsible for secure application design and development receive appropriate training regarding Netlify's secure application development practices.

I. SECURE CODE REVIEW. Netlify performs a combination of static and dynamic testing of code prior to the release of such code. Vulnerabilities are addressed in accordance with its current software vulnerability management program.

J. ILLICIT CODE. The Services do not knowingly contain viruses, malware, worms, date bombs, time bombs, shut-down devices, that may result in, either: (a) any inoperability of the Services; or (b) any interruption, interference with the operation of the Services (collectively, "Illicit Code").

6. No Backdoors into the Services.

Netlify has not built any backdoors into the Services which would allow government authorities to access Customer Data.

7. Physical Security Measures

On an annual basis, Netlify evaluates the security measures implemented by its data center hosting providers.

8. Organizational Security Measures

A. PERSONNEL SECURITY. Netlify performs background screening on all employees and all contractors who have access to Personal Data in accordance with Netlify's applicable standard operating procedure and subject to Applicable Data Protection Laws.

B. SECURITY AWARENESS AND TRAINING. Netlify maintains a security and privacy awareness program that includes appropriate training and education of Netlify personnel, including any contractors or third parties that may access Personal Data. Such training is conducted at time of hire and at least annually thereafter throughout employment at Vendor.

C. VENDOR RISK MANAGEMENT. Netlify maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Personal Data for appropriate security and privacy controls and business disciplines.

D. SOFTWARE AND ASSET INVENTORY. Netlify maintains an inventory of all software components (including, but not limited to, open source software) used in the Services, and inventory of all media and equipment where Personal Data is stored.

E. WORKSTATION SECURITY. Netlify implements and maintains security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption. Netlify restricts personnel from disabling security mechanisms. Personal Data is not permitted to be stored on workstations or any portable storage device without explicit permission.

F. CRYPTOGRAPHIC CONTROLS. Netlify hashes all passwords using a minimum of SHA 256. Netlify has implemented a high availability architecture for storing cryptographic keys.