Netlify Data Processing Agreement

Last Updated: September 12, 2021
Prior Version: May 17, 2021

This Data Protection Addendum ("DPA") forms part of the Principal Agreement entered into between Netlify, Inc. (“Netlify”) and Customer (as defined herein).

By signing this DPA, Customer enters into this DPA acting on its own behalf and, to the extent required under Applicable Data Protection Laws, as agent for each Customer Affiliate.

In consideration of the mutual obligations set out herein with respect to the Processing and securityof Personal Data under the Principal Agreement, the parties hereby agree that the terms and conditions set out below shall be added as a DPA to the Principal Agreement.

Capitalized terms not otherwise defined herein shall have the meaning given to them in thePrincipal Agreement.

In the event of a conflict between the terms and conditions of this DPA and the Principal Agreement with respect to the Processing and security of Personal Data, the terms and conditions of this DPA shall govern and control. In the event of a conflict between the terms of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

This DPA includes 2 parts:

1) the main body of the DPA, and

2) Exhibit 1 - “Standard Contractual Clauses” and its Appendix that includes Annex I (data exporter’s details of the transfer), Annex II (data importer’s technical and organisational security measures), and Annex III (list of Sub-processors).

To execute this DPA that has been pre-signed by Netlify, Customer must complete the following steps:

a. Complete the “Customer” information on page 9 and sign; and
b. Email the completed and signed DPA to privacy@netlify.com.

Upon receipt of the validly completed DPA by Netlify at this email address, this DPA will become legally binding.

The parties agree as follows:

1. Definitions

1.1. **"Anonymous Data"** means Personal Data that has been processed in such a manner that itcan no longer be attributed to an identified or identifiable natural person.

1.2. **"Applicable Data Protection Laws"** means all laws and regulations, including laws and regulations of the European Union and the European Economic Area and their member states, Switzerland, the United Kingdom, and California, applicable to the Processing of Personal Data under the Principal Agreement.

1.3. **"Affiliate"** means any entity that owns or controls, is owned or controlled by, or is under common control or ownership with a party to this DPA, where control is defined as the direct or indirect ownership or control of more than 50% of the voting interests of the entity.

1.4. **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., including any amendments and any implementing regulations thereto that become effectiveon or after the effective date of this DPA.

1.5. **"Controller"** means the entity that alone or jointly with others, determines the purposes andmeans of the Processing of Personal Data. For the purposes of this DPA only, the term Controller shall include Controller Affiliates.

1.6. **"Customer"** means the entity identified as such as a signatory to this DPA, and identified as"Customer" or "User" in the Principal Agreement. For the purposes of this DPA only, the term "Customer" shall include Customer Affiliates.

1.7. **"Customer Personal Data**" means any Personal Data Processed by Netlify on behalf of aCustomer pursuant to or in connection with the Principal Agreement.

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

1.9. **"Delete"** means to remove or obliterate Personal Data such that it cannot be recovered orreconstructed.

1.10. **"GDPR"** means EU General Data Protection Regulation 2016/679.

1.11. **"Personal Data"** means any information relating to Data Subject which is subject to the Applicable Data Protection Laws and which Processor Processes on behalf of Controllerother than Anonymous Data.

1.12. **"Principal Agreement"** means Netlify's Terms of Service Agreement, SaaS Services Agreement, Order Form or any other written or electronic agreement for the purchase of services from Netlify (identified as "Services" in the applicable agreement or order form),which Customer has signed up for and agreed to, including Netlify's Privacy Policy.

1.13. **"Processor"** means the entity, including its Affiliates which Processes Personal Data onbehalf of the Controller.

1.14. **"Services"** means the services and other activities to be supplied to or carried out by or onbehalf of Netlify for Customer pursuant to the Principal Agreement.

1.15. **"Standard Contractual Clauses"** means the contractual clauses attached hereto as Exhibit1 pursuant to the European Commission's decision of 2021/914 of 4 June 2021 and its Module

2 (Controller to Processor) for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection.

1.16. **“Sub-processor”** means any Processor engaged by or on behalf of Netlify or any NetlifyAffiliate to Process Personal Data on behalf of Customer pursuant to the Principal Agreement.

1.17. The terms, **"Commission", "Personal Data Breach"**, **"Process"**, **"Processing"** and **"Supervisory Authority"** shall have the same meaning as in the GDPR.

2. Processing of Customer Personal Data

2.1. Roles of the Parties**:**

The parties acknowledge and agree that with respect to the Processing of Personal Data,Customer is the Controller and Netlify is the Processor. This DPA does not apply to Personal Data for which Netlify is a Controller.

2.2. Netlify shall:

2.2.1. comply with all Applicable Data Protection Laws in the Processing of CustomerPersonal Data;

2.2.2. process the Personal Data only on documented instructions from the Controller or asset forth in the Principal Agreement and/or Exhibit 1 Annex I of this DPA, unless Processing is required by Applicable Data Protection Laws to which Netlify is subject, in which case Netlify shall to the extent permitted by Applicable Data Protection Laws inform the Controller of that legal requirement before the relevant Processing of that Personal Data;

2.2.3. as soon as reasonably practicable upon becoming aware, inform Customer if, inNetlify’s opinion, an instruction from Customer infringes the GDPR or other Applicable Data Protection Laws;

2.2.4. take steps to ensure that any natural person acting under the authority of Netlify whohas access to Personal Data does not Process them except on instructions from the Customer, unless he or she is required to do so by Applicable Data Protection Laws; and

2.2.5. take reasonable steps to ensure that access to Customer Personal Data is limited to authorized personnel who need to know or have access to the relevant Customer Personal Data as necessary to perform the Services pursuant to the Principal Agreement, ensuring that all such individuals are appropriately trained and informedof the confidential nature of Personal Data and have committed themselves to confidentiality.

2.3. Customer:

2.3.1. shall comply with all Applicable Data Protection Laws in its role as Controller ofand in its Processing of Customer Personal Data;

2.3.2. warrants and represents that:

2.3.2.1. it has a valid lawful basis or bases under Applicable Data Protection Lawsfor its Processing of Personal Data;

2.3.2.2. that it has the sole responsibility for the accuracy and legality of PersonalData, and the means by which it acquired such Personal Data; and

2.3.2.3. that it has the right to transfer or provide access to Personal Data to Netlify asreasonably necessary for the provision of Services under the Principal Agreement;

2.3.3. instructs Netlify to:

2.3.3.1. Process Customer Personal Data; and

2.3.3.2. in particular, transfer Customer Personal Data to any country or territory, as reasonably necessary for the provision of Services pursuant to the Principal Agreement; and

2.3.4. warrants and represents that its instructions to Netlify for the Processing of PersonalData comply with Applicable Data Protection Laws, and that Processing of PersonalData in accordance with Customer's instructions will not cause Netlify to be in breach of any Applicable Data Protection Laws.

3. Details of the Processing

3.1. Exhibit 1 Annex I to this DPA sets out the duration, nature and purpose of Netlify's Processing, the types of Personal Data and categories of Data Subjects that Netlify Processes as required bythe GDPR. The subject matter of Processing of Personal Data by Netlify is the performance of Services pursuant to the Principal Agreement.

3.2. Netlify shall not Process Personal Data (i) for purposes other than those set forth in the Principal Agreement and/or Exhibit I Annex I of this DPA, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by the supervisory authority to which Netlify is subject; in such a case, Netlify shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and (iii) in violation of the Applicable Data Protection Laws. Customer hereby instructs Netlify to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Customer in its use of Services.

3.3. Customer may make reasonable amendments to Exhibit 1 Annex I by written notice to Netlify from time to time as Customer reasonably considers necessary to meet its requirements. Nothing in Exhibit 1 Annex I (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this DPA.

4. Security

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope,

context and purposes of Processing as well as the risk of varying likelihood and severity forthe rights and freedoms of natural persons, Netlify shall in relation to Customer Personal Data maintain appropriate technical and organizational measures to ensure a level of

security appropriate to the risks that are presented by Processing of Customer Personal Data,including protection against accidental or unlawful destruction, loss, alteration, unauthorizeddisclosure of, or access to Customer Personal Data transmitted, stored or otherwise in Netlify's possession or under its control. Such measures include the measures specified in Exhibit 1 Annex II of this DPA.

5. Sub-processing

5.1. Customer acknowledges and agrees that Netlify may utilize the authorized Sub-processorsset forth in Exhibit 1 Annex III. Customer can subscribe to receive email notification of updates to Sub-processors by submitting (i) the email address for such notifications and (ii) the full name of the subscribing legal entity, if applicable.

5.2. Netlify shall by email inform Customer who has subscribed to receive notifications of any changes concerning the addition or replacement of sub-processors, at least ten (10) business days prior to such change(s), thereby giving Customer the opportunity to object to such changes. Customer may object in writing to Netlify's intended change concerning Netlify's Sub-processors within five (5) business days of such notice.

5.3. If it is not possible for Netlify and Customer to resolve the issue within a reasonable time despite both parties' good faith efforts, notwithstanding anything in the Principal Agreement, Customer may suspend or terminate the Principal Agreement to the extent thatit relates to Services which require the use of the proposed Sub-processor.

5.4. Netlify will enter into a written agreement with each Sub-processor containing terms whichoffer at least the same level of protection for Customer Personal Data as those set out in thisDPA, imposing in particular that each Sub-processor provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR.

5.5. Netlify shall remain fully liable to Customer for the performance of its Sub-processor's obligations to the same extent Netlify would be liable if performing the Services directlyunder the terms of this DPA.

5.6. If Customer and Netlify have entered into Standard Contractual Clauses as described in Section 11 (Transfer Mechanisms for Data Transfers), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Netlify of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Sub-processors that must be provided by Netlify to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Netlify beforehand, and that such copies will be provided by the Netlify only upon request by Customer.

6. Data Subject Rights

Netlify shall, to the extent permitted by Applicable Data Protection Laws to which Netlify is subject, promptly notify Customer if Netlify receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, right to erasure ("right to

be forgotten"), right to restriction or cessation of processing, right to data portability, withdrawal of consent to Processing, right to object to the Processing of Data Subject's Personal Data for direct marketing purposes, right to object to Processing based on GDPR Article 6 (1) (e) or (f), or the Data Subject's right not to be subject to a decision based solelyon automated processing (such requests individually and collectively, "Data Subject Request(s)").

6.1. If Netlify receives a Data Subject Request in relation to Customer's data, Netlify will advisethe Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure,restriction or cessation of Processing, or withdrawal of consent to Processing of any Personal Data are communicated to Netlify, and, if applicable, for ensuring that a record of consent to Processing is maintained with respect to each Data Subject.

6.2. Netlify shall, at the request of Customer, and taking into account the nature of the Processing, assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respondto Data Subject Requests; provided that (i) Customer is itself unable to respond without Netlify's assistance and (ii) Netlify is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for anycosts and expenses arising from any such assistance by Netlify.

7. Personal Data Breach

7.1. Taking into account the nature of the Processing and the information available to Netlify,Netlify shall:

7.1.1. notify Customer without undue delay after becoming aware of a Personal Data breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet its obligations under Applicable Data Protection Laws to reportor inform Data Subjects or a supervisory authority of the Personal Data breach; and

7.1.2. co-operate with Customer and take such reasonable commercial steps as are directedby Customer to assist in the investigation, mitigation and remediation of each such PersonalData breach.

7.2. The obligations described in Section 7.1 shall not apply in the event that a Personal Data breach results from the actions or omissions of Customer. Netlify's obligation to report or respond to a Personal Data breach under Section 7.1 will not be construed as an acknowledgement by Netlify of any fault or liability with respect to the Personal Data breach.

8. Data Protection Impact Assessment and Prior Consultation

To the extent required under the GDPR, Netlify shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, which Customer

reasonably considers to be required of Customer under the GDPR or equivalent provisions of any other Applicable Data Protection Laws. In each case, the reasonable assistance provided by Netlify, shall be solely in relation to Processing of Customer Personal Data pursuant to the Principal Agreement and taking into account the nature of the Processing and the information available to Netlify. Customer shall be responsible to the extent legallypermitted for any costs and expenses arising from any such assistance by Netlify.

9. Deletion or return of Customer Personal Data

9.1. At Customer's request or following the termination or expiration of the Principal Agreement, Netlify shall return Customer Data to Customer and, to the extent allowed byApplicable Data Protection Laws, delete Customer Personal Data.

10. Audit Rights

10.1. To the extent required by the GDPR, with reasonable notice, Netlify shall make available to Customer on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of Customer Personal Data by Netlify. Customer must conduct its audits during normal business hours and take every reasonable precaution to avoid any unnecessary disruption to Netlify's operations. Customershall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Netlify for any time expended for on-site audits. If Customer and Netlify have entered into Standard Contractual Clauses as described in Section 11 (Transfer Mechanisms for Data Transfers), the parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with this Section 10.1.

10.2. Netlify shall maintain records sufficient to demonstrate its compliance with its obligationsunder this DPA and retain such records for a period of three (3) years after the terminationof the Principal Agreement.

10.3. Netlify shall immediately notify Customer if an instruction, in Netlify's opinion, infringesthe Applicable Data Protection Laws or supervisory authority requirements.

11. Transfer Mechanisms for Data Transfers

11.1 The parties agree that Netlify may transfer Personal Data processed under this DPA outsidethe European Economic Area or Switzerland as necessary to provide Services. To provide appropriate safeguards, the following transfer mechanisms shall apply under this DPA to any transfers of Personal Data to countries which do not ensure an adequate level of data protection within the meaning of the Applicable Data Protection Laws: Standard Contractual Clauses, set forth in Exhibit 1.

11.2 To the extent Customer transfers Personal Data from the United Kingdom to Netlify by signing this DPA, Customer and Netlify conclude the UK Standard Contractual Clauses annexed to EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, which are hereby incorporated by reference and completed as follows: (i) the "data exporter" is Customer and the "data importer" is Netlify; (ii) the governing law in Clause 9 and Clause 11.3 is the law of the country in which Customer is established; (iii) Appendix 1 and Appendix 2 are Annex I and Annex II to this DPA respectively, and (iv) the optional indemnification clause is not applicable. In addition, the following changes apply: (i) references to Data Protection Law are replaced with references to applicable UK data protection law; (ii) references to the EU or Member States are replaced with references to the United Kingdom, (iii) references to EU authorities are replaced with references to the

competent UK authority; and (iv) references to the Member State governing law in Clause 9 and Clause 11.3 are replaced with references to the law of England and Wales.

12. Government and Law Enforcement Requests

12.1 Upon receipt of any legally binding order or request for disclosure of Personal Data by a competent government authority or law enforcement authority, Netlify shall use reasonable efforts to redirect the relevant authority to Customer pursuant to Clause 15 of the Standard Contractual Clauses. Customer agrees that Netlify can provide information to such relevant authority as reasonably necessary to redirect the order or request. In the event Netlify is prohibited by applicable laws from notifying Customer of the relevant authority's request or order, Netlify shall use reasonable efforts to challenge such request or order.

13. Data Protection Officer

13.1. Netlify has appointed a data protection officer ("DPO") who may be reached atprivacy@netlify.com.

13.2. Customer will provide Netlify with contact information for its DPO or similar personauthorized to respond to inquiries regarding Processing of Customer Personal Data.

14. CCPA

14.1. The parties acknowledge and agree that Netlify is a service provider for the purposes of theCCPA and is receiving personal information from Customer pursuant to the Principal Agreement for a business purpose. Netlify shall not sell any such personal information. Netlify shall not retain, use or disclose any personal information provided by Customer pursuant to the Principal Agreement except as necessary for the specific purpose of performing the services for Customer pursuant to the Principal Agreement, or otherwise as set forth in the Principal Agreement or as permitted by the CCPA. For the purposes of this Section 14.1, the terms "personal information," "service provider," "sale," and "sell" are asdefined in Section 1798.140 of the CCPA. Netlify certifies that it understands the restrictions of this Section 14.1.

15. General Terms

Governing law and jurisdiction

15.1. Without prejudice to Clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction) of the Standard Contractual Clauses:

15.1.1. the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising underthis DPA.

Limitation of liability

15.2. The total liability of each of Customer and Netlify (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this

DPA,whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Principal Agreement.

Netlify's role as a Controller

15.3. The parties acknowledge and agree that to the extent Netlify processes Personal Data in connection with the Principal Agreement to: (i) monitor, prevent and detect fraud, and to prevent harm to Customer, Netlify and Netlify's affiliates, and to third parties; (ii) comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Netlify is subject; (iii) analyze, develop and improve Netlify's products and services; or (iv) provide Netlify's products and services to Netlify users, Netlify is acting as a Controller with respect to the Processing of such Personal Data it receives from or through Customer.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

CUSTOMER

Signature  Name Elke Heinemann

Title Owner Date Signed 06.02.2023

NETLIFY, INC.

Signature DocuSigned by:  B716DA8C729E4C6... Name Matt Biilmann

Title CEO Date Signed 10/13/2021

EXHIBIT 1: STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties: (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions: (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7; (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e); (iii) Clause 9(a), (c), (d) and (e); (iv) Clause 12(a), (d) and (f); (v) Clause 13; (vi) Clause 15.1(c), (d) and (e); (vii) Clause 16(e); (viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

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 specified in Annex I.B.

Clause 7 - Optional

Docking clause

Not applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without

prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 2: GENERAL WRITTEN AUTHORIZATION. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to: (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13; (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract,

insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO EXHIBIT 1 STANDARD CONTRACTUAL CLAUSES
ANNEX I

A. LIST OF PARTIES

Data exporter: The data exporter is the (i) legal entity that has created an account with Netlify, Inc. ("Netlify") for provision of Services, and executed the Clauses as a data exporter and, (ii) all affiliates of such entity established within the EEA, which have purchased Services from Netlify or its Affiliates.

Data importer: The data importer is Netlify, which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the Principal Agreement between the data exporter and Netlify.

B. DESCRIPTION OF TRANSFER

Data subjects: The data exporter may submit Personal Data to Netlify and its Affiliates 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 thedata 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);and/or
- Natural persons authorized by the data exporter to use the services provided by Netlify, Inc.to the data exporter.

Categories of data: The data exporter may submit Personal Data to Netlify, Inc. and its Affiliates which may include,but is not limited to, the following categories of Personal Data: Names, titles, position, employer,contact information (email, phone, fax, physical address etc.), identification data, profession life data, personal life data, connection data, or localization data (including IP addresses).

Special categories of data (if appropriate): None

Processing operations: The objective of the processing of Personal Data by Netlify is to provide Services, pursuant to the Principal Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority/ies with responsibility for data exporter's compliance with Regulation

(EU) 2016/679 as regards the data transfer. This information shall be made available to Netlify on request.

APPENDIX TO EXHIBIT 1 STANDARD CONTRACTUAL CLAUSES

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

In processing Personal Data, the Data Importer represents and warrants that it has implemented andwill maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Netlify Services, as described in security documentation at http://netlify.com/security or otherwise made reasonably available by Data Importer. Data Importer will not materially decrease the overall security of Services during the term of the Principal Agreement.

APPENDIX TO EXHIBIT 1 OF STANDARD CONTRACTUAL CLAUSES

ANNEX III

LIST OF SUB-PROCESSORS

The current list of Sub-processors for Services is provided below:

Name	Purpose	Location
Fivetran	Analytics	United States
Segment	Analytics	United States
Google Analytics	Analytics	United States
Zuora	Billing	United States
Dropbox	Contracts	United States
Salesforce	Customer relationship management	United States
Intercom	Customer support	United States
Zendesk	Customer support	United States
Discourse (Community)	Customer Support platform	United States
Census	Data automation	United States
DMARCian	DMARC report processing	United States
Typeform	Feedback forms	United States
Askimet	Form and Wordpress Spam protection	United States
Sift	Fraud account detection	United States
Amazon Web Service (AWS)	Infrastructure service provider	United States
Digital Ocean	Infrastructure service provider	United States
Google Cloud	Infrastructure service provider	United States
Microsoft Azure	Infrastructure service provider	United States
Packet	Infrastructure service provider	United States
Rackspace	Infrastructure service provider	United States
Yandex	Infrastructure service provider	United States
Google Suite	Legal documents such as DPA	United States
Humio	Logs	United States
Hubspot	Marketing	United States
MailChimp	Marketing and transactional email	United States
Braintree	Payment processing	United States
FullStory	Session tracking	United States