COVER PAGE

Attached please find Webflow, Inc. ("Webflow")'s Data Processing Agreement ("DPA") addressing the parties' obligations and rights in relation to the processing of personal data. This DPA forms part of the Services Agreement or other written agreement between you and Webflow.

To complete this DPA, we request that you:

1. *Complete the information in the signature box on p. 9*
2. *If signing manually outside of the automated HelloSign process, please send the completed document and signed DPA to Webflow by email to dpa@webflow.com.*

If you have questions about this DPA, please contact Webflow support or email dpa@webflow.com.

WEBFLOW’S DATA PROCESSING AGREEMENT

This Data Processing Agreement (“DPA”) is entered into between Webflow, Inc. (“Webflow”) and Customer (jointly “the Parties”), and forms a part of the Services Agreement between the Parties, and reflects the Parties’ agreement with regard to the Processing of Personal Data in accordance with the requirements of the Data Protection Laws.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Webflow processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

This DPA is effective on the date that it has been duly executed by both Parties (“Effective Date”), and amends, supersedes and replaces any prior data processing agreements that the Parties may have been entered into. Any modifications to the terms of this DPA (whether handwritten or otherwise) will render this DPA ineffective unless Webflow has separately agreed to those modifications in writing.

1. Definitions

1.1. “Affiliate” means any entity that directly or indirectly controls, is controlled by or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. “Authorized Affiliate” means Customer's Affiliate(s) which (a) are 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; (b) are permitted to use the Services pursuant to the Agreement between Customer and Webflow; and (c) have not signed their own Services Agreement with Webflow and are not "Customers" as defined under this DPA.

1.3. “Covered Services” or “Services” means the services that are ordered by the Customer from Webflow involving the Processing of Personal Data on behalf of the Customer.

1.4. “Customer” means the entity that signed the Services Agreement and that determines the purposes and means of Processing of Personal Data. The Customer is considered the “Controller” of the Personal Data provided pursuant to this DPA.

1.5. “Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer’s Personal Data transmitted, stored or otherwise Processed.

1.6. “Data Protection Laws” means any applicable law, statute, law, regulation or order by governmental authority of competent jurisdiction, or any judgment, decision, decree, injunction, writ, order, subpoena, or like action of any court, arbitrator or other government entity, and at all times during the term of the Service Agreement, including the laws of the European Union (“EU”), the UK Data Protection Act 2018, the EU General Data Protection Regulation ("GDPR"), and the California Consumer Privacy Act and its accompanying regulations ("CCPA"), all as amended or replaced from time to time, and any other foreign or domestic laws to the extent that they are applicable to a party in the course of its performance of the Contract.

1.7. "Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject') that is subject to the GDPR or the laws of non-EU EEA countries that have formally adopted the GDPR, which is provided by or on behalf of Customer and Processed by Webflow pursuant to the Services Agreement.

1.8. "Regulator" means any supervisory authority with authority under Data Protection Laws over all or any part of the provision or receipt of the Services or the Processing of Personal Data.

1.9. "Services Agreement" means any Terms of Service agreement (also available at https://webflow.com/legal/terms) between Webflow and Customer under which Covered Services are provided by Webflow to Customer.

1.10. "Standard Contractual Clauses" means the annex found in the European 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 of the European Parliament and of the Council* (available as of 23 July, 2020 at data.europa.eu/eli/dec/2010/87/oj).

1.11. "Subprocessor" means any Processor engaged by Webflow to Process Personal Data on behalf of Webflow.

1.12. Terms such as "Data Subject", "Processing", "Controller", "Processor" and "Supervisory Authority" shall have the meaning ascribed to them in the Data Protection Laws.

2. Services Agreement

2.1. This DPA supplements the Services Agreement and in the event of any conflict between the terms of this DPA and the terms of the Services Agreement, the terms of this DPA prevail with regard to the specific subject matter of this DPA.

3. Data Protection Laws

3.1. **Roles of the Parties.** The Parties acknowledge and agree that Webflow will Process the Personal Data in the capacity of a Processor and that Customer will be the Controller of the Personal Data.

3.2. **DPO.** The Parties, to the extent required by the GDPR, will each designate a data protection officer (a "DPO") and provide their contact details to the other Party where required by the Data Protection Laws.

4. Obligations of the Controller

4.1. **Instructions.** Customer warrants that the instructions it provides to Webflow pursuant to this DPA will comply with Data Protection Laws.

4.2. **Data Subject and Regulator Requests.** Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under Data Protection Laws and all communications from Regulators that relate to the Personal Data, in accordance with Data Protection Laws. To the extent such requests or communications require Webflow's assistance, Customer shall immediately notify Webflow in writing of the Data Subject's or Regulator's request.

4.3. **Notice, Consent and Other Authorizations.** Customer agrees that the Personal Data will be collected in compliance with Data Protection Laws, including all legally required consents, approvals and authorizations. Upon Webflow's request, Customer shall provide adequate proof of having properly obtained all such necessary consents, authorizations and required permissions.

5. Details of Processing Activities

5.1. The following table sets out the details of Processing:

Purposes for which the Personal Data shall be processed	● Webflow will process Personal Data for the purpose of providing the Covered Services described in the Services Agreement. Customer may submit Personal Data to the Services, and may request for its users ("End Users") to submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion
Description of the categories of the data subjects	● Natural persons who submit personal data to Customer via use of the Services; ● Natural persons who are employees, representatives, or other business contacts of Customer
Description of the categories of Personal Data	● Personal data processed includes: name, email address, phone number, credit card and/or other billing information; ● Personal data about End Users that Customer provides to the Service or through your End User's interaction with the Services; ● Personal data from Add-ons and other third-party services you use in conjunction with our Services; ● Data about Customers and End Users' use of the Services, such as but not limited to interactions with the user interface to the Services, and the Internet Protocol Address for the computers with which you use to connect to the Service.
Description of special categories of Personal Data	● Website visitors or end users may submit special categories of Personal Data to the Customer via the Services, the extent of which is determined and controlled by the Customer. For clarity, these special categories of Personal Data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs.

6. Obligations of the Processor

6.1. **Scope of Processing**. Webflow will Process the Personal Data on documented instructions from Customer in such manner as is necessary for the provision of Services under the Service Agreement, except as may be required to comply with any legal obligation to which Webflow is subject. Webflow may make reasonable effort to inform Customer if, in its opinion, the execution of an instruction relating to the Processing of Personal Data could infringe on any Data Protection Laws. In the event Webflow must Process or cease Processing Personal Data for the purpose of complying with a legal obligation, Webflow will inform the Customer of that legal requirement before Processing or ceasing to Process, unless prohibited by the law.

6.2. **Data Subject and Regulator Requests**. Webflow will promptly notify Customer in writing of any complaints, questions or requests received from Data Subjects or Regulators regarding the Personal Data. Taking into account the nature of the Processing and to the extent reasonably possible, Webflow will assist Customer in fulfilling Customer's obligations in relation to Data Subject requests under applicable Data Protection Laws.

6.3. **Retention**. Upon Customer's written request Webflow will destroy all Personal Data in its possession or return the Personal Data to Customer, as requested. Notwithstanding the foregoing, any return or destruction shall be subject to all applicable laws, regulations and Webflow's compliance policies.

6.4. **Disclosure to Third Parties**. Except as expressly provided in this DPA, Webflow will not disclose Personal Data to any third party without Customer's consent. If requested or required by a competent governmental authority to disclose the Personal Data, to the extent legally permissible and practicable, Webflow will provide Customer with sufficient prior written notice in order to permit Customer the opportunity to oppose any such disclosure.

6.5. **Confidentiality**. Webflow will restrict access to the Personal Data to its personnel (and the personnel of its Affiliates) and to its Subprocessors who need access to meet Webflow's obligations under the Services Agreement. Further, Webflow will ensure that all such personnel and Subprocessors are informed of the confidential nature of the Personal Data and have undertaken training on how to handle such data. Webflow will ensure that personnel authorized to Process the Personal Data are subject to binding confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

6.6. **GDPR Articles 32-36**. Taking into account the nature of the Processing and the information available to Webflow, Webflow will provide reasonable assistance to Customer in complying with its obligations under GDPR Articles 32-36, which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation.

6.7. **Information Security**. Taking into account the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, Webflow will take appropriate steps to implement and maintain adequate organizational and technical measures designed to protect the confidentiality, integrity and availability of the Personal Data it Processes on Customer's behalf (the "Security Measures"). All of the Personal Data Webflow processes is stored in the cloud. Webflow uses only cloud providers that have confirmed they have implemented and maintain Security Measures in compliance with Article 32 of the GDPR, in storing and keeping secure Personal Data. For more details about Webflow's security measures, please see Annex 2.

7. Audit

7.1. **Scope**. Webflow will maintain records of its Processing activities as required by the Data Protection Laws and will make available to Customer that is not a competitor of Webflow information reasonably necessary to demonstrate its compliance with the obligations set out in this DPA. Customer's inspection rights under this DPA do not extend to Webflow's employee payroll, personnel records or any portions of its sites, books, documents, records, or other information that do not relate to the Services or to the extent they pertain to third parties.

7.2. **Process**. Subject to reasonable written notice from Customer and at the Customer's additional expense (including all reasonable costs and fees for any and all time Webflow expends on such audit, in addition to the rates for services performed by Webflow), Webflow and Customer shall mutually agree to appoint a third-party auditor to verify that Webflow is in compliance with the obligations under this DPA. In no event shall the Parties agree to a third-party auditor that is a competitor to Webflow. Audits and inspections will be carried out at mutually agreed times during regular business hours, and no more than once per calendar year. The Parties shall mutually agree upon the duration of the audit.

7.3. **Confidentiality**. All information obtained during any such request for information or audit will be considered Webflow's confidential information under the Services Agreement and this DPA. The results of the inspection and all information reviewed during such inspection will be deemed Webflow's confidential information. The third party auditor may only disclose to Customer specific violations of this DPA if any, and the basis for such findings, and shall not disclose any of the records or information reviewed during the inspection.

8. Contracting with Subprocessors

Customer hereby consents to Webflow's engagement of Subprocessors in connection with the processing of the Personal Data. A list of Webflow's current Subprocessors ("Subprocessor's List") is located at https://webflow.com/legal/subprocessors. Customer may reasonably object to any new Subprocessor within 15 days of receiving notice, in which case Webflow will use reasonable efforts to make a change in the Service or recommend a commercially reasonable change to avoid processing by such Subprocessor. If Webflow is unable to provide an alternative, Customer may terminate the Services and will pay Webflow any fees or expenses not yet paid for all services provided pursuant to any Services Agreement. Webflow will enter into written agreements with each Subprocessor containing reasonable provisions relating to the implementation of technical and organizational measures in compliance with the GDPR. In relation to Customer, Webflow will remain liable for acts and omissions of its Subprocessors in connection with the provision of the Services.

9. Transfers Outside of the European Economic Area

9.1. Customer acknowledges that Webflow may, without Customer's prior written consent, transfer the Personal Data to a foreign jurisdiction provided such transfer is either (i) to a country or territory which has been formally recognized by the European Commission as affording the Personal Data an adequate level of protection or (ii) the transfer is otherwise safeguarded by mechanisms, such as Standard Contractual Clauses and other certification instruments, recognized and approved by the European Commission from time to time.

9.2. **Standard Contractual Clauses.** If Customer's use of the Services involves Customer's transfer of Personal Data from the United Kingdom or EEA to Webflow, or if entering into the Standard Contractual Clauses set forth in Annex 1 to this DPA with Webflow would otherwise help Customer satisfy a legal obligation relating to the international transfer of Personal Data, then (i) by entering into this DPA, the Parties are deemed to be signing such Standard Contractual Clauses, including each of its applicable Appendices and (ii) such Standard Contractual Clauses form part of this DPA and take precedence over any other provisions of this DPA to the extent of any conflict.

9.3. **Privacy Shield.** Webflow is certified with the terms of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. The Parties acknowledge and agree that on the request of the United States Department of Commerce (or any successor body) or a competent supervisory authority, enforcement or other public or regulatory authority, court or tribunal, Webflow may make available to them a summary or representative copy of this Agreement or any relevant provisions in the Agreement.

10. Information Obligations and Incident Management

10.1. **Data Breach**. Webflow will notify Customer of any Data Breach of which it becomes aware without undue delay consistent with measures necessary to determine the scope of the breach and to restore the integrity of Webflow's systems. Webflow will use reasonable efforts to investigate the Data Breach and take any actions that are reasonably necessary to mitigate damage, as required by law and as appropriate under the circumstances.

10.2. **Notification**. Webflow's notification of a Data Breach, to the extent known, will include: (a) the nature of the Data Breach; (b) the date and time upon which the Data Breach took place and was discovered; (c) the number of Data Subjects affected by the incident; (d) the categories of Personal Data involved; (e) the measures – such as encryption, or other technical or organizational measures – that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) the name and contact details of the data protection officer or other contact; and (g) a description of the likely consequences of the Data

Breach.

10.3. **Coordination**. Webflow will reasonably assist Customer in fulfilling its obligations to notify Data Subjects and the relevant authorities in relation to a Data Breach, provided that nothing in this section shall prevent either Party from complying with its obligations under Data Protection Laws. The Parties agree to coordinate in good faith on developing the content of any related public statements.

11. Obligations Post- Termination

Termination or expiration of this DPA shall not discharge the Parties from their obligations that by their nature may reasonably be deemed to survive the termination or expiration of this DPA.

12. Liability and Indemnity

Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Services Agreement.

13. Severability

Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt in good faith to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this Agreement.

The Parties' authorized signatories have duly executed this DPA.

Signed
for and on behalf of the Customer

Dina Maier

Print name: Dina Maier

Customer email: info@kuechenzauber.de

Company name: Küchenzauber

Title: Geschäftsleitung

Date: 2020 / 12 / 17

Signed
for and on behalf of Webflow

Print name: **Vlad Magdalin**

Title: **CEO**

Date: **23 June 2020**

Annex 1

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Customer (as identified, with contact information, in the main part of the DPA above)

Other information needed to identify the organisation: N/A

(the data **exporter**)

And

Name of the data importing organisation: Webflow, Inc.

Address: 398 11th Street, 2nd Floor, San Francisco, CA 94103

E-mail: privacy@webflow.com

Other information needed to identify the organisation: N/A

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[2]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

[2] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
Customer, user of the Covered Services described in the Services Agreement.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
Webflow, Inc., provider of the Covered Services described in the Services Agreement.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
Natural persons who submit personal data to Customer via use of the Services; and
Natural persons who are employees, representatives, or other business contacts of Customer.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Personal data processed includes:

- name, email address, phone number, credit card and/or other billing information;
- Personal data about End Users that Customer provides to the Services or through an End User's interaction with the Services;
- Personal data from Add-ons and other third-party services Customer uses in conjunction with the Services;
- Data about Customers and End Users' use of the Services, such as but not limited to interactions with the user interface to the Services, and the Internet Protocol Address for the computers used to connect to the Service.

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

Website visitors or end users may submit special categories of Personal Data to the Customer via the Services, the extent of which is determined and controlled by the Customer. For clarity, these special categories of Personal Data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs.

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

Webflow will process Personal Data for the purpose of providing the Covered Services described in the Services Agreement. The specific processing activities are within the Customer's control but are anticipated to include receiving, storing, displaying, and erasing Personal Data.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Annex 2 to the DPA below.

Annex 2

Security Policies, Procedures, Controls

Webflow implements the following security measures with respect to the Personal Data:

1. Data Center Security
   a. Webflow infrastructure is managed via Amazon Web Services' ISO 27001 certified data centers, and hosted in multiple regions and availability zones.
   b. All database servers are isolated inside virtual private networks, and accessible only by key personnel via multi-factor authentication.
   c. All access to production environments is logged, and access can be immediately revoked.
2. Protection from Data Loss and Corruption
   a. All data operations are mirrored to a redundant secondary database.
   b. All data is backed up on a daily basis, and stored on highly-redundant storage media in multiple availability zones.
   c. All data is encrypted at rest using Amazon's EBS encryption functionality.
3. Application Level Security
   a. User account passwords are hashed using a secure low-entropy key derivation function, which protects against brute-force attacks.
   b. All applications are served exclusively via TLS with a modern configuration.
   c. All login pages have brute-force logging and protection.
   d. Two-factor authentication is supported, and is mandatory for all internal administrator functions of the application.
   e. All code changes to our applications require code reviews via an enforced code review process.
   f. Automated code and dependency analysis tools are in place to identify emergent security issues.
   g. Regular application security penetration tests are conducted by different vendors. These tests include high-level server penetration tests across various parts of our platform (i.e. Dashboard, Designer, Editor, Hosted Sites), as well as security-focused source code reviews.
4. Internal Protocol & Training
   a. All new employees are given security and data privacy training, tailored to their job functions.
   b. All employees undergo regular security best practices and data privacy training.
   c. All developers undergo advanced application security and privacy training.
   d. All new product changes and improvements undergo a data privacy assessment before any projects proceeds to implementation.

HELLOSIGN

Audit Trail

TITLE	Signature request from Webflow, Inc.
FILE NAME	Webflow Data Processing Agreement.pdf
DOCUMENT ID	27fa132f32be4e544d5a3e0eddbfd7c2fdd49632
AUDIT TRAIL DATE FORMAT	YYYY / MM / DD
STATUS	● Completed

Document History

SENT	**2020** / **12** / **17** 08:22:13 UTC-8	Sent for signature to Dina Maier (info@kuechenzauber.de) from signatures@webflow.com IP: 52.6.82.82
VIEWED	**2020** / **12** / **17** 08:22:31 UTC-8	Viewed by Dina Maier (info@kuechenzauber.de) IP: 78.94.131.245
SIGNED	**2020** / **12** / **17** 08:25:52 UTC-8	Signed by Dina Maier (info@kuechenzauber.de) IP: 78.94.131.245
COMPLETED	**2020** / **12** / **17** 08:25:52 UTC-8	The document has been completed.