

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”) Data Protection Act 1998, the EU General Data Protection Regulation (“GDPR”), 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 agreement executed by and between the Customer and Webflow, and attached as Annex 3 pursuant to the European Commission’s decision of 5 February 2010 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in third countries to which do not ensure an adequate level of data protection, and any new Standard Contractual Clauses applicable between controllers and processors issued after the Agreement’s effective date.
- 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.
- 2.2. Any provisions contained in this DPA that would not apply to the Parties but for the GDPR shall not apply to the Parties until May 25, 2018 and thereafter.

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.** Upon enforcement of the GDPR, 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> 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.** Upon enforcement of the GDPR, and 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 1.

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. **Privacy Shield.** Webflow is certified with the terms of the EU-U.S. and Swiss - U.S. Privacy Shield Frameworks and such certification will serve as the transfer mechanisms for any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to the United States. 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 invalidating 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



Print name: David Ranftler

Customer email: hello@davidran.me

Company name: N/A

Title: Product Researcher

Date: 2020 / 03 / 08

Signed
for and on behalf of Webflow



Print name: **Vlad Magdalin**

Title: **CEO**

Date: **2018/05/22**

Annex 1

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.

TITLE	Signature request from Webflow, Inc.
FILE NAME	Webflow Data Proc...Agreement (1).pdf
DOCUMENT ID	44967ad9347b033b0856314c5f2d611f7c6e2020
AUDIT TRAIL DATE FORMAT	YYYY / MM / DD
STATUS	● Completed

Document History



SENT

2020 / 03 / 08

10:02:19 UTC-8

Sent for signature to David Ranftler (hello@davidran.me)
 from signatures@webflow.com
 IP: 3.220.22.251



VIEWED

2020 / 03 / 08

10:02:38 UTC-8

Viewed by David Ranftler (hello@davidran.me)
 IP: 89.1.215.211



SIGNED

2020 / 03 / 08

10:03:32 UTC-8

Signed by David Ranftler (hello@davidran.me)
 IP: 89.1.215.211



COMPLETED

2020 / 03 / 08

10:03:32 UTC-8

The document has been completed.