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 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 Data Protection Laws; (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. "CCPA" means the California Consumer Privacy Act of 2018 (California Civil Code sections 1798.100 - 1798.199) and its accompanying regulations.

1.4. "Controller" means the entity that determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, Customer is the Controller. For the purposes of this DPA, all references to Controller shall also mean "business" as defined in the CCPA for CCPA purposes.

1.5. "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.

1.6. "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.

1.7. "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.

1.8. "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 Services Agreement, including the laws of the European Union, the UK Data Protection Act 2018, the GDPR, and the 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 Services Agreement.

1.9. "Data Subject" means either: 1) the individual within the European Economic Area and the United Kingdom to whom Personal Data relates for GDPR purposes, or 2) a "consumer," as such term is defined in the CCPA for CCPA purposes

1.10. "GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.11. "Personal Data" means either: 1) data about a specific natural person within the European Economic Area or the United Kingdom from which that person is identified or identifiable, as defined in GDPR or 2) "personal information" as defined in the CCPA for CCPA purposes, which is provided by or on behalf of Customer and Processed by Webflow pursuant to the Services Agreement.

1.12. "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.13. "Processor" means the entity which Processes Personal Data on behalf of the Controller. For purposes of this DPA, Webflow, including its Affiliates, is the Processor. For the purposes of this DPA, all references to Processor shall also mean "service provider" as defined in the CCPA for CCPA purposes.

1.14. "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.

1.15. "Services Agreement" means any services agreement including, but not limited to, Webflow's online terms (available at webflow.com/legal/terms) between Webflow and Customer under which Covered Services are provided by Webflow to Customer.

1.16. "Standard Contractual Clauses" means the annex found in the European Commission decision of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* (available as of August 1, 2021 at data.europa.eu/eli/dec_impl/2021/914/oj).

1.17. "Sub-processor" means any Processor engaged by Webflow to Process Personal Data on behalf of Webflow.

2. Services Agreement

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 Data Protection Laws.

4. Controller Obligations

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 it collects shall be in accordance with Data Protection Laws, including all legally required consents, bases of processing, approvals, and authorizations. Upon Webflow's request, Customer shall provide all information necessary to demonstrate compliance with these requirements.

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 the Customer's End User's interaction with the Services; • Personal data from add-ons and other third-party services the Customer uses in conjunction with our Services; • Data about Customers and End Users' use of the Services, including, but not limited to, interactions with the user interface to the Services, web browser or operating system details, and the Internet Protocol Address for the computers with which Customers and End Users use to connect to the Services.
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, trade union membership, biometric data, health data, or data concerning a natural person's sex life or sexual orientation.

6. Processor Obligations Supplementing the Standard Contractual Clauses

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. **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.

6.3. **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.

7. Audit

7.1. **Scope**. Webflow will maintain records of its Processing activities carried out on behalf of Customer and will make available to Customer the information reasonably necessary to demonstrate its compliance with the obligations set out in this DPA. Webflow may limit the scope of information made available to Customer if Customer is a Webflow competitor, provided that such limitation does not violate Data Protection Laws or the Standard Contractual Clauses. 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 thirty (30) days prior 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. Customer shall be entitled to exercise this audit right no more than once every twelve (12) months. Customer shall not be entitled to an on-site audit of Webflow's premises without demonstrating a compelling need for such an on-site audit. 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 Sub-processors

Customer hereby gives its general authorisation for Webflow to engage new Sub-processors in connection with the processing of the Personal Data as set forth in clause 9 of the Standard Contractual Clauses. A list of Webflow's current Sub-processors is located at webflow.com/legal/subprocessors. Customer must sign up at the aforementioned URL to receive email notifications concerning the addition of new Sub-processors. Customer may reasonably object to the addition of any new Sub-processor within 15 calendar days of receiving such email notification, 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 Sub-processor. If Webflow is unable to provide an alternative, Customer may terminate the Services and shall pay Webflow any fees or expenses not yet paid for all services provided pursuant to any Services Agreement. If Customer fails to sign up for these email notifications, Customer shall be deemed to have waived its right to object to the newly added Sub-processor(s).

9. Transfers Outside of the European Economic Area

9.1. **Transfer.** 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 European Economic Area to Webflow, or if entering into the Standard Contractual Clauses set forth in the Appendix 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 Annexes 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 as of August 1, 2021. 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 DPA or any relevant provisions in the DPA.

10. Additional Terms for California Data Subjects

To the extent that the CCPA applies, Webflow agrees it will not: (a) sell California Data Subjects' Personal Data (as "sell" is defined in the CCPA); (b) retain, use, or disclose California Data Subjects' Personal Data for a commercial purpose other than providing the services specified in the Services Agreement; (c) retain, use, or disclose California Data Subjects' Personal Data outside of the direct business relationship between Processor and Customer.

Webflow certifies that it understands these restrictions set out in this section and will comply with them.

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

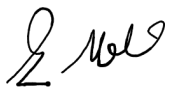
Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Services Agreement.

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



Print name: Yannik Moll

Customer email: team@growably.de

Company name: Growably UG (haftungsbeschränkt)

Title: Geschäftsführer

Date: 2022 / 03 / 14

Signed
for and on behalf of Webflow

Print name: **Vlad Magdalin**

Title: **CEO**

Date: 2021 / 08 / 01

APPENDIX

STANDARD CONTRACTUAL CLAUSES

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)[1] 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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 the 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[4] (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.

[2] [INTENTIONALLY OMITTED]

[3] [INTENTIONALLY OMITTED]

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION: 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 fifteen (15) calendar 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.[8] 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

[5] [INTENTIONALLY OMITTED]
[6] [INTENTIONALLY OMITTED]
[7] [INTENTIONALLY OMITTED]
[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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

MODULE TWO: Transfer controller to processor

(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.

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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

MODULE TWO: Transfer controller to processor

(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[12];

(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.

[9] [INTENTIONALLY OMITTED]

[10] [INTENTIONALLY OMITTED]

[11] [INTENTIONALLY OMITTED]

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

(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.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter:
Name: Customer, user of the Covered Services.
Contact Details: Specified in the signature block above.
Activities relevant to the data transfer: Use of the Covered Services.
Role: Controller.

Data importer:
Name: Webflow, Inc., provider of the Covered Services.
Contact Details: 398 11th St., Floor 2, San Francisco, CA 94103.
Activities relevant to the data transfer: Provisioning of the Covered Services.
Role: Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred:

- 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 personal data transferred:

- 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; and
- Data about Customers and End Users' use of the Services, including, but not limited to, interactions with the user interface to the Services, web browser or operating system details, and the Internet Protocol Address for the computers with which Customers and End Users use to connect to the Services.

Sensitive data transferred (if applicable):

- 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, trade union membership, biometric data, health data, or data concerning a natural person's sex life or sexual orientation.
- Any sensitive data that Customer may submit to Webflow is stored in a single database location with heavily restricted access.

Frequency of the transfer:

- Continuous.

Purposes of the data transfer and further processing:

- 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.

The period for which the personal data will be retained:

- Personal data will be retained during the term of the Services Agreement. Upon the termination of the Services Agreement, the data importer will delete all personal data processed on behalf of the data exporter unless local laws, regulations, or other requirements applicable to the data importer prohibit the deletion of the personal data.

Subject matter, nature, and duration of the processing by sub-processors:

- A list of Webflow's current Sub-processors and the subject matter of the sub-processing can be found at webflow.com/legal/subprocessors. Webflow's Sub-processors process personal data for the term of the agreement between the sub-processor and Webflow.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

- Ireland's Data Protection Commissioner.

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

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

MODULE TWO: Transfer controller to processor

Webflow has a SOC 2 certification and is dedicated to the continued validation of its security program. Specifically, 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.
5. Sub-processor Controls
    a. Webflow only uses 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.

6. Technical and Organisational Measures to provide assistance to the Controller

    a. Webflow has a dedicated security and privacy team to respond to Controller requests and inquiries. Taking into account the nature of the Processing and to the extent reasonably possible, Webflow will assist Controller in fulfilling its obligations in relation to Data Subject requests and compliance obligations under applicable Data Protection Laws. This team can be contacted at privacy@webflow.com.

HELLOSIGN

Audit Trail

TITLE	Signature request from Webflow, Inc.
FILE NAME	Webflow Data Processing Agreement.pdf
DOCUMENT ID	ec616ae30415fd7163acf2134f7f1391db674598
AUDIT TRAIL DATE FORMAT	YYYY / MM / DD
STATUS	● Signed

Document History

SENT	**2022 / 03 / 14** 08:35:01 UTC-7	Sent for signature to Yannik Moll (team@growably.de) from signatures@webflow.com IP: 3.90.230.11
VIEWED	**2022 / 03 / 14** 08:36:10 UTC-7	Viewed by Yannik Moll (team@growably.de) IP: 194.8.199.29
SIGNED	**2022 / 03 / 14** 08:38:45 UTC-7	Signed by Yannik Moll (team@growably.de) IP: 194.8.199.29
COMPLETED	**2022 / 03 / 14** 08:38:45 UTC-7	The document has been completed.