Exhibit D - Data Processing Agreement (DPA)

THIS DATA PROCESSING ADDENDUM is made between Prismic.io, Inc. ("**Prismic**"), a Delaware, USA corporation whose principal offices are at 185 Alewife Brook Parkway, #410 Cambridge, MA 02138 USA , and each Prismic customer ("**Customer**") who has entered into a Subscription Agreement (as defined below) with Prismic pursuant to which Prismic and Customer agree to be bound by this Data Processing Addendum.

1. **Introduction**

1.1 Prismic and Customer have entered into a Prismic Master Services Agreement ("**Subscription Agreement**") whereby Prismic has agreed to provide the services to Customer. In connection with the services, Prismic may process personal data for which Customer may be a data controller under the EU Data Protection Laws (as defined below).

1.2 The Customer and Prismic have agreed to enter into this data processing addendum ("**DPA**") in order to ensure that adequate safeguards are put in place with respect to the processing of personal data carried out by Prismic as part of the Subscription Agreement as required by the EU Data Protection Laws.

2. Definitions

2.1 The following expressions are used in this DPA:

"**Adequate Country**" means a country or territory that is recognized under EU Data Protection Laws from time to time as providing adequate protection for personal data;

"**Prismic Group**" means Prismic and any corporate entities which are from time to time under Common Control with Prismic;

"**Prismic Software**" means the computer software applications, tools, application programming interfaces (APIs), connectors, programs, networks and equipment that Prismic uses to make the services available to its customers.

"**EU Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states, applicable to the processing of Personal Data under the Subscription Agreement, including (where applicable) the GDPR;

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of that data;

"**Personal Data**" means all data which is defined and regulated as 'Personal Data' in the EU Data Protection Laws and which is provided by Customer to Prismic or accessed, stored or otherwise processed by Prismic in connection with the services;

"**Prismic Services**" means the Prismic Solution, the Prismic API, the Prismic Software and any other services provided by Prismic as part of the Subscription Agreement;

"**Standard Contractual Clauses**" ("SCCs") means the standard contractual clauses for the transfer of personal data to third countries approved by the European Commission in the decision (EU) 2021/914 of 4 June 2021;

"**processing**", "**data controller**", "**data subject**", "**supervisory authority**" and "**data processor**" will have the meanings ascribed to them in the EU Data Protection Laws.

2.2 An entity **"Controls"** another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other

shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2.3 All terms not defined in this DPA shall have the same meaning as defined in the Subscription Agreement.

3. Status of the parties

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

3.2 As between the parties, Customer is solely responsible for obtaining, and represents and covenants that it has obtained and will obtain, all necessary consents, licenses and approvals for the processing, or otherwise has a valid legal basis under EU Data Protection Laws for the Processing of any Personal Data as part of the Services. Each of Customer and Prismic warrant in relation to Personal Data that it will comply with (and will ensure that any of its staff and/or subcontractors comply with), the EU Data Protection Laws; provided, however, that Prismic's warranty is subject to Customer's compliance with the obligations in this Section 3.2.

3.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties acknowledge and agree that Customer is the Data Controller and Prismic is the Data Processor. Prismic agrees that it will process all Personal Data in accordance with its obligations pursuant to this DPA.

3.4 Each of Prismic and Customer will notify to each other one or more individuals within its organisation authorised to respond from time to time to enquiries regarding the Personal Data and each of Prismic and Customer will deal with those enquiries promptly.

4. **Prismic obligations**

4.1 With respect to all Personal Data, Prismic agrees that it will:

(a) only process the Personal Data for the purposes described in Exhibit 1 and will act only in accordance with this DPA and Customer's written instructions. This DPA, and Customer's use of the Prismic software's features and functionality, are Customer's written instructions to Prismic in relation to the processing of personal data. Customer agrees that Prismic will have no liability under the Subscription Agreement to the extent Prismic's compliance with any Customer instruction hinders Prismic's ability to provide the Prismic Services;

(b) in the unlikely event that applicable law requires Prismic to process Personal Data other than pursuant to Customer's instructions, Prismic will notify Customer (unless prohibited from so doing by applicable law);

(c) without undue delay upon becoming aware, inform Customer if, in Prismic's opinion, any instructions provided by Customer under Clause 3.1(a) infringe the EU Data Protection Laws;

(d) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data in Prismic's possession or under its control. Those measures include the security measures specified in Appendix III of the SCCs below.

(e) ensure that its personnel have access to Personal Data only as necessary to perform the Prismic services in accordance with the Subscription Agreement and this DPA, and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality;

(f) notify Customer without undue delay after becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Prismic's possession or under its control (including when transmitted, stored or otherwise processed by Prismic) (a "**Security Breach**");

(g) taking into account the nature of the processing, promptly provide Customer with reasonable cooperation and assistance in respect of the Security Breach and all information in Prismic's possession concerning the Security Breach, including, to the extent known to Prismic, the following:

(i) the possible cause and consequences of the Security Breach;

(ii) the categories of Personal Data involved;

(iii) a summary of the possible consequences for the relevant data subjects;

(iv) a summary of the unauthorised recipients of the Personal Data; and

(v) the measures taken by Prismic to mitigate any damage;

(h) Prismic will return Personal Data to Customer by permitting Customer to export Personal Data from the Prismic Services at any time during provision of the Prismic Services, using the Prismic software's then existing features and functionality. Customer may delete Customer Data at any time. Prismic will delete the Personal Data within 30 days of termination or expiration of the Term of the Subscription Agreement. Prismic will provide a certificate of deletion at Customer's request. Prismic is not obligated to delete copies of Personal Data retained in automated backup copies generated by Prismic, which Prismic will retain for up to, and delete within, 3 months from their creation. Any backup copies will remain subject to this DPA and the Subscription Agreement until they are destroyed.

(j) taking into account the nature of processing and the information available to Prismic, assist Customer when reasonably requested in relation to Customer's obligations under EU Data Protection Laws with respect to:

(i) data protection impact assessments (as that term is defined in the GDPR);

(ii) notifications to the supervisory authority under EU Data Protection Laws and/or communications to data subjects by Customer in response to any Security Breach; and

(iii) Customer's compliance with its obligations under the GDPR with respect to the security of processing.

(k) taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, to respond to data subjects' requests to exercise their rights under Chapter III of the GDPR. Prismic will promptly notify Customer of requests received by Prismic, unless otherwise required by applicable law. Customer may make changes to Personal Data processed with the Prismic Services using the features and functionality of the Prismic Software. Except as required by law, Prismic will not make changes to that data except as agreed in writing with Customer.

5. **Sub-processing**

5.1 Prismic will not disclose or transfer Personal Data to any third party without the prior written notification of Customer, except (i) as specifically stated in this Agreement, or (ii) where the disclosure or transfer is required by any applicable law, regulation, or public authority.

5.2 Customer consents to Prismic's use of sub-processors (a "**Sub-processor**") to provide aspects of the Prismic Services, and to Prismic's disclosure and provision of Personal Data to those sub-processors. Prismic sub-processors are listed in Exhibit 1. Prismic will require its Sub-processors to comply with terms that are substantially no less protective of Personal Data than those imposed on Prismic in this DPA (to the extent applicable to the services provided by the Sub-processor). Prismic will be liable for any breach of its obligations under this DPA that is caused by an act, error or omission of a Sub-processor. Customer may authorize new Sub-processors, provided that:

(a) Prismic provides notice to Customer of the aspects of the Prismic Services concerned, the name and contact details of any new Sub-processor to process Personal Data in connection with its provision of Prismic Services;

(b) Prismic requires each Sub-processor to comply with terms which are substantially no less protective of Personal Data than those imposed on Prismic in this DPA, to the extent reasonably applicable to the services that Sub-processor provides.

5.3 The Customer has a period of 15 days from the date of receipt of Prismic's notice to submit its legitimate and justifiable objections on reasonable data protection grounds regarding the use of any future Sub-processor. In the absence of notification of objections after this period, the Customer shall be deemed to have authorized the use of the relevant Sub-processor. If Customer objects to the authorization of any future Sub-processor within the above time period, and if Prismic is unable to provide an alternative or workaround solution to avoid processing of Personal Data by the objected Sub-processor within a reasonable period of time, not exceeding 30 days from receipt of the objection, then, at any time within expiration of that 30 days period, Customer may elect to terminate the processing of Personal Data under affected sales orders to the Subscription Agreement without penalty, by notice to Prismic to that effect. If Customer terminates Prismic Services in accordance with the foregoing, then Prismic will refund to Customer a pro-rata amount of any affected Prismic Services fees prepaid to Prismic and applicable to the unutilized portion of the subscription term for terminated Prismic Services.

6. Audit and records

6.1 Prismic will, in accordance with EU Data Protection Laws, make available to Customer any information in Prismic's possession or control as Customer may reasonably request with a view to demonstrating Prismic's compliance with the obligations of data processors under EU Data Protection Law in relation to its processing of Personal Data.

6.2 Prismic conducts regular third-party audit of the compliance of its Prismic Services with EU Data Protection Law. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligation set forth in the Subscription Agreement, Prismic shall make available to Customer information regarding Prismic's compliance with the obligations set forth in this DPA in the form of a copy of Prismic's then most recent third-party audits. Such audit, to the extent not made generally publicly available by Prismic on its website, constitute Prismic's confidential information.

7. Data transfers

7.1 To the extent any processing of Personal Data by Prismic takes place in any country outside the EEA (other than exclusively in an Adequate Country), the parties agree that the SCCs as set out in Exhibit 2 will apply in respect of that processing and Prismic will comply with the obligations of the 'data importer' in the SCCs and Customer will comply with the obligations of 'data exporter'.

7.2 The Customer acknowledges and agrees that the provision of the Prismic Services under the Subscription Agreement may require the processing of Personal Data by Sub-processors in countries outside the EEA from time to time.

7.3 If, in the performance of this DPA, Prismic transfers any Personal Data to a Sub-processor (or any member of the Prismic Group that acts as a Sub-processor) and without prejudice to clause 5 where the Sub-processor will process Personal Data outside the EEA (other than exclusively in an Adequate Country), Prismic will in advance of any transfer ensure that a mechanism to achieve adequacy in respect of that processing is in place including:

(a) the requirement for Prismic to execute SCCs approved by the EU authorities under EU data Protection Laws as set out in Exhibit 2;

(b) the existence of any other specifically approved safeguard for data transfers (as recognised under the EU Data Protection Laws) and/or a European Commission finding of adequacy.

7.4 If Prismic receives any requests for access to Personal Data from public authorities, Prismic shall made its best efforts to:

(a) review the legality of any order to disclose Personal Data, including whether the order is within the remit of the powers granted to the requesting authority;

(b) challenge the order if, after assessment, Prismic concludes that there are grounds under applicable laws to do so;

(c) when challenging an order, seek interim measures to suspend the effect of the order until a decision is made by relevant courts on the challenge to the order;

(d) not disclose any Personal Data requested until required to do so under applicable procedural rules;

(e) inform the requesting public authority that the order is incompatible with the safeguards contained in the Standard Contractual Clauses and there is therefore a conflict of obligations for Prismic;

(f) where it is legally permitted to do so, Prismic shall notify the Customer that the order has been received as soon as possible;

(g) where necessary to disclose Personal Data, having followed the steps set out in this Clause 7.4, only provide the minimum amount of Personal Data permissible when responding to the order, based on a reasonable interpretation of the order.

8. Customer obligations

8.1 Customer undertakes to:

(a) provide Prismic with the Personal Data mentioned in Exhibit 1, to the exclusion of any improper, disproportionate or unnecessary Personal Data, and to the exclusion of any "particular" Personal Data as defined in the GDPR;

(b) collect under its liability, lawfully, fairly and in a transparent manner the Personal Data provided to Prismic, for the performance of Prismic Services, and in particular, to ensure the lawfulness of processing and the information due to the data subjects;

(c) maintain a record of processing activities carried out and more generally, comply with the principles of the EU Data Protection Laws;

(d) ensure, before and throughout the processing, compliance with the obligations set out in the EU Data Protection Laws;

(e) not provide to Prismic any "particular" Personal Data as defined in the GDPR.

9. Prismic Liability

Prismic's liability under or in connection with this DPA shall be subject to the exclusions and liability caps set forth in the Subscription Agreement.

10. General

10.1 This DPA is without prejudice to the rights and obligations of the parties under the Subscription Agreement which will continue to have full force and effect. This DPA is incorporated into and made a part of the Subscription Agreement by this reference. In the event of any conflict between the terms of this DPA and the terms of the Subscription Agreement, the terms of this DPA will prevail so far as the subject matter concerns the processing of Personal Data.

10.2 Customer and Prismic each agree that the dispute resolution provisions of the Subscription Agreement (including governing law and venue) apply to this DPA.

EXECUTED as of the date of the Subscription Agreement (the "**Effective Date**")

DATA EXPORTER	DATA IMPORTER
	Prismic.io Inc
Name:	Name: Sadek DRODI
Title :	Title: CEO
Authorized Signature	Authorized Signature

Exhibit 1

1.1. Details of the Personal Data and Processing Activities

Purpose(s) of the processing	Provide the Prismic Services (i.e. content management system services / building, hosting, maintenance and support of customized websites and apps)
Nature of the processing	Collection, storage, disclosure by transmission, erasure
Categories of Personal Data	Customer may submit Personal Data to the Prismic Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data : Identification data (i.e. first name, last name, email), Connection data (i.e. encrypted password, IP address), Professional data (i.e. job), Content published or uploaded in websites and apps
Categories of Data subjects	Users of the Prismic Services Visitors of the Customer's websites and/or apps
Duration of the processing	Duration of the Subscription Agreement plus three months

1.2. Third Party Sub-processors

Prismic Subprocessors List pub-rev10-202106-cnt

Entity	Location	HQ	Prismic use it as part of
Algolia	FR (EU)	55 Rue d'Amsterdam, 75008 Paris, France	Core Services
Amazon Inc.	USA	1200 12th Avenue South Suite 1200 Seattle, WA 98144	Core Services
Amazon Inc.	USA	1200 12th Avenue South Suite 1200 Seattle, WA 98144	Hosting Services
Datadog	USA	620 8th Avenue, Floor 45 New York, NY 10018	Quality Assurance
Docusign, Inc.	USA	221 Main St., Suite 1550 San Francisco, CA 94105	Sales
elastic.io GmbH	DE (EU)	elastic.io GmbH Quantiusstraße 21 53115 Bonn	Core Services
Functional Software, Inc.	USA	132 Hawthorne Street San Francisco, CA 94107 United States	Quality Assurance

Google LLC	**USA**	1600 Amphitheater Parkway, Mountain View, CA 94043, USA	Website Visitors Writing Room (inactive)
Google LLC	**USA**	1600 Amphitheater Parkway, Mountain View, CA 94043, USA	Customer Support Accounting Marketing & Sales Employees
Hubspot, Inc	**USA**	25 1st Street Cambridge, MA 02141 USA	Customer Support Marketing & Sales
Intercom, Inc.	**USA**	55 2nd Street 4th Floor San Francisco, CA 94105	Customer Support Marketing
MixPanel Inc.	**USA**	405 Howard Street, 2nd Floor, San Francisco, CA 94105	Core Services
Sendgrid, Inc.	**USA**	1801 California Street, Suite 500, Denver, CO 80202, USA	Core Services Signup Marketing & Sales
Stripe, Inc.	**USA**	3180 18th Street San Francisco, CA 94110 United States	Accounting
Zebrafish Labs, Inc	**USA**	1141 Howard Street San Francisco, CA 94103 United States	Core Services

1.3 Prismic Group Sub-processors

New Prismic, SAS	**France (EU)**	9 rue de la Pierre Levée 75011 PARIS	Core Services, Marketing & Sales, Accounting, Customer Support, Quality Assurance, Signup

Exhibit 2

2021 EU Model clauses extracted from Annex to the Commission implementing decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (UE) 2016/679 of the European Parliament and of the Council

---

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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b);

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

Clause 4

Interpretation

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

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

(e) 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

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.

8.1 Instructions

(f) 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.

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout

the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) 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 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

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

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

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

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

importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

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

(h) The Parties agree that those shall be the courts of France.

(i) 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.

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

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The Customer that has subscribed to the data importer's online content platform-as-a-service solution.

Address: See the Subscription Agreement

Contact person's name, position and contact details: *Data Protection Contact* as set forth in the Subscription Agreement

Activities relevant to the data transferred under these Clauses: Performance of the Prismic Services pursuant to the Subscription Agreement

Signature and date:

Role : Controller

Data importer(s):

Name: Prismic.io, Inc.

Address: 185 Alewife Brook Parkway, #410 Cambridge, MA 02138 USA

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Performance of the Prismic Services pursuant to the Subscription Agreement

Signature and date:

Role : Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of the Prismic Services and Visitors of the Data exporter's website and/or apps

Categories of personal data transferred

Customer may submit Personal Data to the Prismic Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data : Identification data (i.e. first name, last name, email), Connection data (i.e. encrypted password, IP address), Professional data (i.e. job), Content published or uploaded in websites and apps

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

There is no sensitive data transferred.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

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

Nature of the processing

Collection, storage, disclosure by transmission, erasure

Purpose(s) of the data transfer and further processing

Provide the Prismic Services (i.e. content management systems services, building, hosting and support of customized websites and apps)

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Duration of the Subscription Agreement plus three months

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The Sub-processor will process Personal Data as necessary to perform the Prismic Services. The Sub-processor will process Personal Data for the duration of the Subscription Agreement, unless otherwise agreed in writing.

See Exhibit 1 for identities of the Sub-processors used for the provision of the Prismic Services and their country of location.

C. COMPETENT SUPERVISORY AUTHORITY

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.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The Data Importer currently abides by the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the term of the applicable Services Agreement.

Hosting Infrastructure. Infrastructure. The Data Importer hosts its services in distributed, secure data centers operated by Amazon Web Services (AWS). Redundancy. The services are replicated across multiple data centers within a geographic region to eliminate single points of failure using an active/passive configuration in order to minimize the impact of environmental risks. Monitoring. The services are protected by automated monitoring which is designed to detect a variety of failure conditions and which will, when appropriate, trigger failover mechanisms. Backups. Backups are performed on a regular basis and stored in a secondary site within the same geographic region. Business Continuity. The Data Importer replicates its service and data over multiple data centers within a geographic region (when made available by Data Importers infrastructure as a service providers) to protect against loss of service or data. The Data Importer conducts periodic tests of failover and data backup procedures to ensure readiness for business continuity and disaster recovery.

Networks & Transmission. Network Data Transmission. Interactions between users, administrators and Data Importer modules are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols. Network Security. The Data Importer employs multiple layers of DOS protection, Intrusion Detection, Rate Limiting and other network security services from both its hosting providers and third party providers. Encryption Technologies. The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available.

Policies and Procedures. Policies. The Data Importer has written, approved policies governing Account Management, Acceptable Use, Data Retention, Employee Code of Conduct, Encryption, Incident Response, Information Sensitivity, Use of Mobile Devices, Password Protection, Patch Management and Risk Management. Procedures. The Data Importer has written and approved procedures for Data Breach Notification, Change Management, Communication, Disaster Recovery, DoS Response, System Backup and Recovery, and Monitoring. Security Response. The Data Importer monitors a variety of communication channels for security incidents, and the Data Importer's security personnel are required to react promptly to known incidents.

Access Controls. Access Procedures. The Data Importer maintains formal access procedures for allowing its personnel access to the production service and components involved in building the production service. Only authorized employees are allowed access to these restricted components and all access is approved by an employee's manager and service owner. Only a small number of individuals are approved to access the restricted components. Audit records are maintained to indicate who has access to restricted components. Access Mechanisms. Access to the Data Importer's production service and build infrastructure occurs only over a secured channel and requires two-factor authentication. Logging. Access to the Data Importer's production service and build infrastructure is done using unique IDs and is logged. Infrastructure Security Personnel. The Data Importer maintains several security policies governing its personnel. The Data Importer's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure, the review of the Services, and responding to security incidents.

Data Protection. In Transit. Interactions between users, administrators and Prismic modules are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols. At Rest. The Data Importer uses cryptographic hashing and encryption mechanisms to protect sensitive information such as cryptographic keys and application secrets. Redundancy. The Data Importer stores data in a multi-tenant

environment within the Data Importer's hosted infrastructure. The data and service are replicated across multiple hosted datacenters within the same geographic region. Data Isolation. The Data Importer logically isolates the Data Exporter's data, and the Data Exporter has a large degree of control over the specific data stored in the Service. Data Deletion. The Data Importer provides to the Data Exporter a mechanism that can be used to delete the Data Exporter's data.

Software Code Review. The Data Importer employs a code review process to improve the security of the code used to provide the Services. All changes to the service are reviewed and approved by a senior engineer other than the author of the change. Automated testing. Each software build is subjected to a comprehensive suite of automated tests. Security Scan. The Data Importer employs a third party to scan the Service for security vulnerabilities on a periodic basis.

Staff Conduct and Security. Staff Conduct. The Data Importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, usage, compliance and professional standards. Background Checks. The Data Importer conducts reasonably appropriate backgrounds checks as legally permissible and in accordance with applicable local labor law and statutory regulations.

Subprocessor Security. Prior to onboarding sub-processors that will handle any data provided by a Data Exporter, the Data Importer conducts an assessment of the security and privacy practices of the sub-processor to help ensure that the sub-processor provides a level of security and data protection controls appropriate to their access to data and the scope of the services they are engaged to provide.

Data Privacy Office. The Data Privacy Office of the Data Importer can be contacted by the Data Exporter's administrators using the mechanism defined at: https://prismic.io/legal/privacy (or via such other means as may be provided by the Data Importer).

ANNEX III – LIST OF SUB-PROCESSORS

See Exhibit 1.