Data Protection Addendum

The customer agreeing to these terms ("Customer") has entered into an agreement with Prerender and certain of its Affiliates (as applicable, "Prerender") under which Prerender has agreed to provide services to Customer (as amended from time to time, the "Agreement").

This Data Protection Addendum, including its appendices (the "Addendum") will be effective and replace any previously applicable data processing and security terms as of the Addendum Effective Date (as defined below). This Addendum forms part of the Agreement.

1. Definitions

For purposes of this Addendum, the terms below shall have the meanings set forth below. Capitalised terms that are used but not otherwise defined in this Addendum shall have the meanings set forth in the Agreement.

1.1. "Addendum Effective Date" means, as applicable, (a) 25 May 2018, if the parties agreed to this Addendum prior to or on such date; or (b) the date on which the parties agreed to this Addendum, if such date is after 25 May 2018.

1.2. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

1.3. "Audit Reports" has the meaning given in Section 5.4.4.

1.4. "Customer Personal Data" means any personal data contained within the data provided to or accessed by Prerender by or on behalf of Customer or Customer end users in connection with the Services.

1.5. "EEA" means the European Economic Area.

1.6. "EU" means the European Union.

1.7. "European Data Protection Legislation" means the GDPR and other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein and Norway and the United Kingdom, applicable to the processing of Customer Personal Data under the Agreement.

1.8. "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 such data, and repealing Directive 95/46/EC.

1.9. "Information Security Incident" means a breach of Prerender's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data in Prerender's possession, custody or control. "Information Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.10. "Model Contract Clauses" or "MCCs" mean the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

1.11. "Security Documentation" means all documents and information made available by Prerender under Section 5.4.1 (Reviews of Security Documentation).

1.12. "Security Measures" has the meaning given in Section 5.1.1 (Prerender's Security Measures).

1.13. "Services" means the services and/or products to be provided by Prerender to Customer under the Agreement.

1.14. Subprocessors" means third parties authorised under this Addendum to process Customer Personal Data in relation to the Services.

1.15. "Term" means the period from the Addendum Effective Date until the end of Prerender's provision of the Services.

1.16. "Third Party Subprocessors" has the meaning given in Section 9 (Subprocessors).

1.17. "Transfer Solution" means the Model Contract Clauses or another solution that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).

1.18. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this Addendum have the meanings given in the GDPR, and the terms "data importer" and "data exporter" have the meanings given in the Model Contract Clauses.

2. Duration of Addendum

This Addendum will take effect on the Addendum Effective Date and, notwithstanding the expiration of the Term, will remain in effect until, and automatically expire upon, Prerender's deletion of all Customer Personal Data as described in this Addendum.

3. Processing of Data

3.1. Roles and Regulatory Compliance; Authorization.

3.1.1. Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

(a) the subject matter and details of the processing are described in Appendix 1;

(b) Prerender is a processor of that Customer Personal Data under the European Data Protection Legislation;

(c) Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Legislation; and

(d) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

3.1.2. Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Prerender that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Prerender as another processor, have been authorised by the relevant controller.

3.2. Scope of Processing.

3.2.1. Customer's Instructions. By entering into this Addendum, Customer instructs Prerender to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services; (b) as authorised by the Agreement, including this Addendum; and (c) as further documented in any other written instructions given by Customer and acknowledged in writing by Prerender as constituting instructions for purposes of this Addendum.

3.2.2. Prerender's Compliance with Instructions. Prerender will only process Customer Personal Data in accordance with Customer's instructions described in Section 3.2.1 (including with regard to data transfers) unless European Data Protection Legislation to which Prerender is subject requires other processing of Customer Personal Data by Prerender, in which case Prerender will notify Customer (unless that law prohibits Prerender from doing so on important grounds of public interest).

4. Data Deletion

4.1. Deletion on Termination. On expiry of the Term, Customer instructs Prerender to delete all Customer Personal Data (including existing copies) from Prerender's systems in accordance with applicable law as soon as reasonably practicable, unless applicable law requires otherwise.

5. Data Security

5.1. Prerender's Security Measures, Controls and Assistance.

5.1.1. Prerender's Security Measures. Prerender will implement and maintain technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Data as described in Appendix 2 (the "Security Measures"). Prerender may update or modify the Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

5.1.2. Security Compliance by Prerender Staff. Prerender will grant access to Customer Personal Data only to employees, contractors and Subprocessors who need such access for the scope of their performance, and are subject to appropriate confidentiality arrangements.

5.1.3. Prerender's Security Assistance. Prerender will (taking into account the nature of the processing of Customer Personal Data and the information available to Prerender) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Customer Personal Data under European Data Protection Legislation, including Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with Section 5.1.1 (Prerender's Security Measures);

(b) complying with the terms of Section 5.2 (Information Security Incidents); and

(c) providing Customer with the Security Documentation in accordance with Section 5.4.1 (Reviews of Security Documentation) and the Agreement, including this Addendum.

5.2. Information Security Incidents

5.2.1. Information Security Incident Notification. If Prerender becomes aware of an Information Security Incident, Prerender will: (a) notify Customer of the Information Security Incident without undue delay after becoming aware of the Information Security Incident; and (b) take reasonable steps to identify the case of such Information Security Incident, minimise harm and prevent a recurrence.

5.2.2. Details of Information Security Incident. Notifications made pursuant to this Section 5.2 (Information Security Incidents) will describe, to the extent possible, details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Prerender recommends Customer take to address the Information Security Incident.

5.2.3. Notification. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Information Security Incident(s).

5.2.4. No Acknowledgement of Fault by Prerender. Prerender's notification of or response to an Information Security Incident under this Section 5.2 (Information Security Incidents) will not be construed as an acknowledgement by Prerender of any fault or liability with respect to the Information Security Incident.

5.3. Customer's Security Responsibilities and Assessment.

5.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Prerender's obligations under Section 5.1 (Prerender's Security Measures, Controls and Assistance) and Section 5.2 (Information Security Incidents):

(a) Customer is solely responsible for its use of the Services, including:

(i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data;

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Services;

(iii) securing Customer's systems and devices Prerender uses to provide the Services; and

(iv) backing up its Customer Personal Data; and

(b) Prerender has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Prerender's and its Subprocessors' systems (for example, offline or on-premises storage).

5.3.2. Customer's Security Assessment.

(a) Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures and Prerender's commitments under this Section 5 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation.

(b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Prerender as set out in Section 5.1.1 (Prerender's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Personal Data.

5.4. Reviews and Audits of Compliance

5.4.1. Customer may audit Prerender's compliance with its obligations under this Addendum up to once per year. In addition, to the extent required by European Data Protection Legislation, including where mandated by Customer's supervisory authority, Customer or Customer's supervisory authority may perform more frequent audits (including inspections). Prerender will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services.

5.4.2. If a third party is to conduct the audit, Prerender may object to the auditor if the auditor is, in Prerender's reasonable opinion, not suitably qualified or independent, a competitor of Prerender, or otherwise manifestly unsuitable. Such objection by Prerender will require Customer to appoint another auditor or conduct the audit itself.

5.4.3. To request an audit, Customer must submit a detailed proposed audit plan to support@prerender.io at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Prerender will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Prerender security, privacy, employment or other relevant policies). Prerender will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 5.4 shall require Prerender to breach any duties of confidentiality.

5.4.4. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor ("Audit Reports") within twelve (12) months of Customer's audit request and Prerender confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

5.4.5. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Prerender's health and safety or other relevant policies, and may not unreasonably interfere with Prerender business activities.

5.4.6. Customer will promptly notify Prerender of any non-compliance discovered during the course of an audit and provide Prerender any audit reports generated in connection with any audit under this Section 5.4, unless prohibited by European Data Protection Legislation or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements

and/or confirming compliance with the requirements of this Addendum. The audit reports are Confidential Information of the parties under the terms of the Agreement.

5.4.7. Any audits are at Customer's expense. Customer shall reimburse Prerender for any time expended by Prerender or its Third Party Subprocessors in connection with any audits or inspections under this Section 5.4 at Prerender's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

5.4.8. The parties agree that this Section 5.4 shall satisfy Prerender's obligations under the audit requirements of the Model Contractual Clauses applied to Data Importer under Clause 5(f) and to any Sub-processors under Clause 11 and Clause 12(2).

6. Impact Assessments and Consultations

Prerender will (taking into account the nature of the processing and the information available to Prerender) reasonably assist Customer in complying with its obligations under European Data Protection Legislation in respect of data protection impact assessments and prior consultation, including, if applicable, Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

6.1. Making available for review copies of the Audit Reports or other documentation describing relevant aspects of Prerender's information security program and the security measures applied in connection therewith; and

6.2. providing the information contained in the Agreement including this Addendum.

7. Data Subject Rights

7.1. Customer's Responsibility for Requests. During the Term, if Prerender receives any request from a data subject in relation to Customer Personal Data, Prerender will advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request. Customer acknowledges and agrees that a Prerender's compliance with any data subjects request in relation to their Personal Data may adversely impact the performance and Customer's use of the Services, and that Customer hereby waives any and all claims of breach, non-performance, loss of data or otherwise, arising from Prerender's compliance with any such request.

7.2. Prerender's Data Subject Request Assistance. Prerender will (taking into account the nature of the processing of Customer Personal Data) provide Customer with self-service functionality through the Services or other reasonable assistance as necessary for Customer to fulfil its obligation under European Data Protection Legislation to respond to requests by data subjects, including if applicable, Customer's obligation to respond to requests for exercising the data subject's rights set out in in Chapter III of the GDPR. Customer shall reimburse Prerender for any such assistance beyond providing self-service features included as part of the Services at Prerender's then-current professional services rates, which shall be made available to Customer upon request.

8. Data Transfers

8.1. Data Storage and Processing Facilities. Prerender may, subject to Section 8.2 (Transfers of Data Out of the EEA), store and process Customer Personal Data anywhere Prerender or its Subprocessors maintains facilities.

8.2. Transfers of Data Out of the EEA.

8.2.1. Prerender's Transfer Obligations. If the storage and/or processing of Customer Personal Data (as set out in Section 8.1 (Data Storage and Processing Facilities)) involves transfers of Customer Personal Data out of the EEA or Switzerland, and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), Prerender will make such transfers in accordance with a Transfer Solution, and make information available to Customer about such Transfer Solution upon request.

8.2.2. Customer's Transfer Obligations. In respect of Transferred Personal Data, Customer agrees that if under European Data Protection Legislation Prerender reasonably requires Customer to enter into Model Contract Clauses or use another Transfer Solution offered

by Prerender, and reasonably requests that Customer take any action (which may include execution of documents) required to give full effect to such solution, Customer will do so.

8.3. Disclosure of Confidential Information Containing Personal Data. If Customer has entered into Model Contract Clauses as described in Section 8.2 (Transfers of Data Out of the EEA), Prerender will, notwithstanding any term to the contrary in the Agreement, make any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, in accordance with such Model Contract Clauses. For the purposes of the Model Contract Clauses, Customer and Prerender agree that (i) Customer will act as the data exporter on Customer's own behalf and on behalf of any of Customer's entities and (ii) Prerender or its relevant Affiliate will act on its own behalf and/or on behalf of Prerender's Affiliates as the data importers.

9. Subprocessors

9.1. Consent to Subprocessor Engagement. Customer specifically authorises the engagement of Prerender's Affiliates as Subprocessors. In addition, Customer generally authorises the engagement of any other third parties as Subprocessors ("Third Party Subprocessors"). If Customer has entered into Model Contract Clauses as described in Section 9.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Prerender of the processing of Customer Personal Data if such consent is required under the Model Contract Clauses.

9.2. Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available in Appendix I (as may be updated by Prerender from time to time in accordance with this Addendum).

9.3. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Prerender will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in the Agreement (including this Addendum) with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Subprocessor. Prerender shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

9.4. Opportunity to Object to Subprocessor Changes.

When any new Third Party Subprocessor is engaged during the Term, Prerender will, at least 30 days before the new Third Party Subprocessor processes any Customer Personal Data, notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform).

Customer may object to any new Third Party Subprocessor by providing written notice to Prerender within ten (10) business days of being informed of the engagement of the Third Party Subprocessor as described above. In the event Customer objects to a new Third Party Subprocessor, Customer and Prerender will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to Prerender.

10. Processing Records

10.1. Prerender's Processing Records. Customer acknowledges that Prerender is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Prerender is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to Prerender, and will ensure that all information provided is kept accurate and up-to-date.

11. Liability

11.1. Liability Cap. The total combined liability of either party and its Affiliates towards the other party and its Affiliates, whether in contract, tort or any other theory of liability, under or in connection

with the Agreement, this Addendum, and the Model Contract Clauses if entered into as described in Section 8.2 (Transfers of Data Out of the EEA) combined will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement, subject to Section 11.2 (Liability Cap Exclusions).

11.2. Liability Cap Exclusions. Nothing in Section 11.1 (Liability Cap) will affect any party's liability to data subjects under the third party beneficiary provisions of the Model Contract Clauses to the extent limitation of such rights is prohibited by the European Data Protection Legislation.

12. Third Party Beneficiary

Notwithstanding anything to the contrary in the Agreement, where Prerender is not a party to the Agreement, Prerender will be a third party beneficiary of Section 5.4 (Reviews and Audits of Compliance), Section 9.1 (Consent to Subprocessor Engagement) and Section 11 (Liability) of this Addendum.

13. Analytics

Customer acknowledges and agrees that Prerender may create and derive from processing related to the Services anonymised and/or aggregated data that does not identify Customer or any natural person, and use, publicise or share with third parties such data to improve Prerender's products and services and for its other legitimate business purposes.

14. Notices

Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Prerender to Customer may be given (a) in accordance with the notice clause of the Agreement; (b) to Prerender's primary points of contact with Customer; and/or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

15. Effect of These Terms

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between this Addendum and the remaining terms of the Agreement, this Addendum will govern.

Appendix 1

Subject Matter and Details of the Data Processing

Subject Matter	Prerender's provision of the Services to Customer.
Duration of the Processing	The Term plus the period from the expiry of the Term until deletion of all Customer Personal Data by Prerender in accordance with the Addendum.
Nature and Purpose of the Processing	Prerender will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Addendum.
Categories of Data	Data relating to individuals provided to Prerender in connection with the Services, by (or at the direction of) Customer.
Data Subjects	Data subjects include the individuals about whom Prerender Processes data in connection with the Services.

Subprocessors

Entity Name	Amazon Web Services, Inc.
Nature and Purpose of the Processing	Prerender's Service is built on Amazon Web Services platform. Amazon Web Services provides all of the physical hardware and infrastructure for Prerender to provide Services to the Customer. Amazon Web Services has access to Customer Personal Data as needed to provide the Prerender Services.
Entity Country	United States

Entity Name	Cloudflare, Inc
Nature and Purpose of the Processing	Cloudflare provides a content distribution network for the Prerender Website. Cloudflare has access to Customer Personal Data for Customer administration of their Prerender Account.
Entity Country	United States

Entity Name	Google Analytics (Google, LLC)
Nature and Purpose of the Processing	Google Analytics is an analytics provider that Prerender uses to capture how users interact with the Prerender website. Google Analytics has access to Customer Personal Data for Customers that visit the Prerender Website.
Entity Country	United States

Entity Name	Stripe, Inc
Nature and Purpose of the Processing	Stripe is an online payment processor that allows Prerender to charge Customer invoices by credit/debit card. Stripe has access to Customer billing information for the sole purpose of billing Customer.
Entity Country	United States

Entity Name	PayPal, Inc
Nature and Purpose of the Processing	PayPal is an online payment processor that allows Prerender to send Customer invoices for payment through the PayPal system. PayPal has access to Customer billing information for the sole purpose of billing Customer.
Entity Country	United States

Appendix 2

Security Measures

As from the Addendum Effective Date, Prerender will implement and maintain the Security Measures set out in this Appendix 2. Prerender may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

Prerender will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Prerender Services. Prerender will not materially decrease the overall security of the Prerender Services during a subscription term.