CLOUDFLARE DATA PROCESSING ADDENDUM

Cloudflare, Inc. ("**Cloudflare**") and the counterparty agreeing to these terms ("**Customer**") have entered into an Enterprise Subscription Agreement, Self-Serve Subscription Agreement or other written or electronic agreement for the Services provided by Cloudflare (the "**Main Agreement**"). This Data Processing Addendum**,** including the appendices (the "**DPA**"**)**, forms part of the Main Agreement.

This DPA will be effective, and will replace and supersede any previously applicable terms relating to their subject matter (including any data processing amendment, agreement or addendum relating to the Services), from the date on which Customer signed or the parties otherwise agreed to this DPA ("**DPA Effective Date**").

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

DATA PROCESSING TERMS

This DPA applies where Cloudflare processes Personal Data as a Processor (or sub-Processor as applicable) on behalf of Customer and such Personal Data is subject to Applicable Data Protection Laws (as defined below).

The parties have agreed to enter into this DPA in order to ensure that appropriate safeguards are in place to protect such Personal Data in accordance with Applicable Data Protection Laws. Accordingly, Cloudflare agrees to comply with the following provisions with respect to any Personal Data that it processes as a Processor (or sub-Processor as applicable) on behalf of Customer.

1. Definitions

1.1 The following definitions are used in this DPA:

a) "**Adequate Country**" means a country or territory that is recognized under European Data Protection Laws as providing adequate protection for Personal Data.

b) "**Affiliate**" means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists).

c) "**Applicable Data Protection Laws**" means all laws and regulations that are applicable to the processing of Personal Data under the Main Agreement, including European Data Protection Laws and the CCPA.

d) "**CCPA**" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 - 1798.199, 2018).

e) "**Cloudflare Group**" means Cloudflare and any of its Affiliates.

f) "**Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

g) "**Customer Group**" means Customer and any of its Affiliates.

h) "**European Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and the United Kingdom applicable to the processing of Personal Data under the Main Agreement (including, where applicable, (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii)).

i) "**Personal Data**" means all data which is defined as '*personal data*', '*personal information*', or '*personally identifiable information*' (or analogous term) under Applicable Data Protection Laws.

j) "**processing**", "**data subject**", and "**supervisory authority**" shall have the meanings ascribed to them in European Data Protection Law.

k) "**Processor**" means an entity which processes Personal Data on behalf of the Controller, including an entity to which another entity discloses a natural individual's personal information for a business purpose pursuant to a written contract that requires the entity receiving the information to only retain, use, or disclose Personal Data information for the purpose of providing the Services.

l) "**Services**" shall refer to all of the cloud-based solutions offered, marketed or sold by Cloudflare or its authorized partners that are designed to increase the performance, security and availability of Internet properties, applications and networks, along with any software, software development kits and application programming interfaces ("**APIs**") made available in connection with the foregoing.

m) "**SCCs**" means: (i) where the EU GDPR or Swiss Federal Act on Data Protection applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 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 ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

n) "**Restricted Transfer**" means: (i) where the EU GDPR or Swiss Federal Act on Data Protection applies, a transfer of Personal Data from the European Economic Area or Switzerland (as applicable) to a country outside of the European Economic Area or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and Information Commissioner (as applicable); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

1.2 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. Status of the parties

2.1 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 Annex 1.

2.2 Each party warrants in relation to Personal Data that it will comply with Applicable Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties acknowledge and agree that the Customer is the Controller (or a Processor processing Personal Data on behalf of a third-party Controller), and Cloudflare is a Processor (or sub-Processor, as applicable).

2.4 If Customer is a Processor, Customer warrants to Cloudflare that Customer's instructions and actions with respect to the Personal Data, including its appointment of Cloudflare as another Processor and, where applicable, concluding the SCCs, have been (and will, for the duration of this DPA, continue to be) authorised by the relevant third-party Controller.

3. Cloudflare obligations

3.1 With respect to all Personal Data it processes in its role as a Processor or sub-Processor, Cloudflare warrants that it shall:

(a) only process Personal Data in order to provide the Service and in accordance with: (i) the Customer's written instructions as set out in the Main Agreement and this DPA, unless required to do so by applicable Union or Member State law to which Cloudflare is subject, and (ii) the requirements of Applicable Data Protection Laws. In the event Cloudflare is required to process Personal Data under Applicable Data Protection Laws, Cloudflare shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) not sell, retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Service, including for a commercial purpose other than providing the Service. Cloudflare shall not use the Personal Data for the purposes of marketing or advertising. Cloudflare's performance of the Service may include disclosing Personal Data to sub-Processors where this is in accordance with Section 4 of this DPA;

(c) inform Customer if, in Cloudflare's opinion, any instructions provided by the Customer under clause 3.1(a) infringe Applicable Data Protection Laws;

(d) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex 2 ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Cloudflare may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Service;

(e) ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under contractual or statutory obligations of confidentiality;

(f) without undue delay notify the Customer upon becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed for the purpose of providing the Services to Customer by Cloudflare, its sub-Processors, or any other identified or unidentified third party (a "**Personal Data Breach**") and provide the Customer with reasonable cooperation and assistance in respect of that Personal Data Breach, including all reasonable information in Cloudflare's possession concerning such Personal Data Breach insofar as it affects the Personal Data;

(g) not make any public announcement about a Personal Data Breach (a "**Breach Notice**") without the prior written consent of the Customer, unless required by applicable law;

(h) to the extent Cloudflare is able to verify that a data subject is associated with the Customer, promptly notify the Customer if it receives a request from a data subject to exercise any data protection rights (including rights of access, rectification or erasure) in respect of that data subject's Personal Data (a "**Data Subject Request**"). Cloudflare shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees;

(i) to the extent Cloudflare is able, and in line with applicable law, provide reasonable assistance to Customer in responding to a data subject request to exercise any data protection rights (including rights of access, rectification or erasure) in respect of that data subject's Personal Data if the Customer does not have the ability to address a Data Subject Request without Cloudflare's assistance. The Customer is responsible for verifying that the requestor is the data subject in respect of whose Personal Data the request is made. Cloudflare bears no responsibility for information provided in good faith to Customer in reliance on this subsection. Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance;

(j) other than to the extent required to comply with applicable law, following termination or expiry of the Main Agreement or completion of the Service, at the choice of Customer, delete or return all Personal Data (including copies thereof) processed pursuant to this DPA;

(k) taking into account the nature of processing and the information available to Cloudflare, provide such assistance to the Customer as the Customer reasonably requests in relation to Cloudflare's obligations under Applicable Data Protection Laws with respect to:

(i) data protection impact assessments and prior consultations (as such terms are defined in Applicable Data Protection Laws);

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

(iii) the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to the security of processing;

provided that the Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance.

4. Sub-processing

4.1 Cloudflare will only disclose Personal Data to sub-Processors for the specific purposes of carrying out the Service. Cloudflare does not sell or disclose Personal Data to third parties for commercial purposes.

4.2 The Customer grants a general written authorization: (a) to Cloudflare to appoint other members of the Cloudflare Group as sub-Processors, and (b) to Cloudflare and other members of the Cloudflare Group to appoint third party data center operators, and business, engineering and customer support providers as sub-Processors to support the performance of the Service.

4.3 Cloudflare will maintain a list of sub-Processors at https://www.cloudflare.com/gdpr/subprocessors/ and will add the names of new and replacement sub-Processors to the list at least thirty (30) days prior to the date on which those sub-Processors commence processing of Personal Data. If Customer objects to any new or replacement sub-Processor on reasonable grounds related to data protection, it shall notify Cloudflare of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If Cloudflare is reasonably able to provide the Service to the Customer in accordance with the Main Agreement without using the sub-Processor and decides in its discretion to do so, then Customer will have no further rights under this clause 4.3 in respect of the proposed use of the sub-Processor. If Cloudflare, in its discretion, requires use of the sub-Processor and is unable to satisfy Customer's objection regarding the proposed use of the new or replacement sub-Processor, then Customer may terminate the applicable Order Form effective upon the date Cloudflare begins use of such new or replacement sub-Processor solely with respect to the Service(s) that will use the proposed new sub-Processor for the processing of Personal Data. If Customer does not provide a timely objection to any new or replacement sub-Processor in accordance with this clause 4.3, Customer will be deemed to have consented to the sub-Processor and waived its right to object.

4.4 Cloudflare will ensure that any sub-Processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-Processor terms (i.e., data protection obligations) that are no less protective of Personal Data than those imposed on Cloudflare in this DPA (the "**Relevant Terms**"). Cloudflare shall procure the performance by such sub-Processor of the Relevant Terms and shall be liable to the Customer for any breach by such sub-Processor of any of the Relevant Terms.

5. Audit and records

5.1 Cloudflare shall, in accordance with Applicable Data Protection Laws, make available to Customer such information in Cloudflare's possession or control as Customer may reasonably request with a view to demonstrating Cloudflare's compliance with the obligations of Processors under Applicable Data Protection Laws in relation to its processing of Personal Data.

5.2 Cloudflare may fulfil Customer's right of audit under Applicable Protection Laws in relation to Personal Data, by providing:

(a) an audit report not older than thirteen (13) months, prepared by an independent external auditor demonstrating that Cloudflare's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard;

(b) additional information in Cloudflare's possession or control to a data protection supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by Cloudflare under this DPA; and

(c) To the extent that Customer's Personal Data is subject to SCCs and the information made available pursuant to this clause 5.2 is insufficient, in Customer's reasonable judgment, to confirm

Cloudflare's compliance with its obligations under this DPA or Applicable Data Protection Laws, then Cloudflare shall enable Customer to request one onsite audit per annual period during the Term (as defined in the Main Agreement) to verify Cloudflare's compliance with its obligations under this DPA in accordance with clause 5.3.

5.3 The following additional terms shall apply to audits the Customer requests:

(a) Customer must send any requests for reviews of Cloudflare's audit reports to compliance@cloudflare.com.

(b) Following receipt by Cloudflare of a request for audit under clause 5.2(c), Cloudflare and Customer will discuss and agree in advance on the reasonable start date, scope, duration of, and security and confidentiality controls applicable to any audit under clause 5.2(c). Whenever possible, evidence for such an audit will be limited to the evidence collected for Cloudflare's most recent third-party audit.

(c) Cloudflare may charge a fee (based on Cloudflare's reasonable costs) for any audit under clause 5.2(c). Cloudflare will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(d) Cloudflare may object in writing to an auditor appointed by Customer to conduct any audit under clause 5.2(c) if the auditor is, in Cloudflare's reasonable opinion, not suitably qualified or independent, a competitor of Cloudflare, or otherwise manifestly unsuitable (i.e., an auditor whose engagement may have a harmful impact on Cloudflare's business comparable to the aforementioned aspects). Any such objection by Cloudflare will require Customer to appoint another auditor or conduct the audit itself. If the SCCs apply, nothing in this clause 5.3 varies or modifies the SCCs nor affects any supervisory authority's or data subject's rights under the SCCs.

6. Data transfers from the EEA, Switzerland, and the UK

6.1 In connection with the Service, the parties anticipate that Cloudflare (and its sub-Processors) may process outside of the European Economic Area ("**EEA**"), Switzerland, and the United Kingdom, certain Personal Data protected by European Data Protection Laws in respect of which Customer or a member of the Customer Group may be a Controller (or Processor on behalf of a third-party Controller, as applicable).

6.2 The parties agree that when the transfer of Personal Data protected by European Data Protection Laws from Customer or any member of the Customer Group to Cloudflare is a Restricted Transfer then it shall be subject to the appropriate SCCs as follows:

(a) in relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply where Customer (or the relevant member of the Customer Group) is a Controller and Module Three will apply where Customer (or the relevant member of the Customer Group) is a Processor;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-Processor changes shall be as set out in Clause 4.3 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 2 will apply, and if the data exporter's Member State does not allow for third-party beneficiary rights, then the law of Germany shall apply;

(vi) in Clause 18(b), disputes shall be resolved before the courts of the jurisdiction governing the Main Agreement between the parties or, if that jurisdiction is not an EU Member State, then the courts in Munich, Germany. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall fall on the country of the governing law;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA; and

(vii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this DPA;

(b) in relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(i) For so long as it is lawfully permitted to rely on the standard contractual clauses for the transfer of Personal Data to Processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between the Customer (or the relevant member of the Customer Group) and Cloudflare on the following basis:

(A) Appendix 1 shall be completed with the relevant information set out in Annex 1 to this DPA;

(B) Appendix 2 shall be completed with the relevant information set out in Annex 2 to this DPA; and

(C) the optional illustrative indemnification clause will not apply.

(ii) Where sub-clause (b)(i) above does not apply, but the Customer (or the relevant member of the Customer Group) and Cloudflare are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

(A) The EU SCCs, completed as set out above in clause 6.2(a) of this DPA, shall also apply to transfers of such Personal Data, subject to sub-clause (B) below;

(B) The UK Addendum shall be deemed executed between the transferring Customer (or the relevant member of the Customer Group) and Cloudflare, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data.

(iii) If neither sub-clause (b)(i) or sub-clause (b)(ii) applies, then Customer and Cloudflare shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK GDPR without undue delay.

(c) in relation to Personal Data that is protected by the Swiss Federal Act on Data Protection (as amended or replaced), the EU SCCs, completed as set out about in clause 6.2(a) of this DPA, shall apply to transfers of such Personal Data, except that:

(i) the competent supervisory authority in respect of such Personal Data shall be the Swiss Federal Data Protection and Information Commissioner;

(ii) in Clause 17, the governing law shall be the laws of Switzerland;

(iii) references to "Member State(s)" in the EU SCCs shall be interpreted to refer to Switzerland, and data subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU SCCs in Switzerland; and

(iv) references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the SCCs shall be understood to be references to the Swiss Federal Act on Data Protection (as amended or replaced).

(d) the following terms shall apply to the SCCs:

(i) Customer may exercise its right of audit under the SCCs as set out in, and subject to the requirements of, clause 5 of this DPA; and

(ii) Cloudflare may appoint sub-Processors as set out in, and subject to the requirements of, clauses 4 and 6.3 of this DPA, and Customer may exercise its right to object to sub-Processors under the SCCs in the manner set out in clause 4.3 of this DPA; and

(e) in the event that any provision of this DPA contradicts, directly or indirectly, the SCCs, the SCCs shall prevail.

6.3 In respect of Restricted Transfers made to Cloudflare under clause 6.2, Cloudflare shall not participate in (nor permit any sub-Processor to participate in) any further Restricted Transfers of Personal Data (whether as an "exporter" or an "importer" of the Personal Data) unless such further Restricted Transfer is made in full compliance with European Data Protection Laws and pursuant to SCCs implemented between the exporter and importer of the Personal Data or an Alternative Transfer Mechanism (as defined in clause 6.5) adopted by the importer applies.

6.4 In the event Customer seeks to conduct any assessment of the adequacy of the SCCs for transfers to any particular countries or regions, Cloudflare shall, to the extent it is able, provide reasonable assistance to Customer for the purpose of any such assessment, provided Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance.

6.5 To the extent Cloudflare adopts an alternative data export mechanism (including any new version of or successor to the Privacy Shield adopted pursuant to applicable European Data Protection Laws) for the transfer of Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Laws and extends to the territories to which Personal Data is transferred), and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to such Alternative Transfer Mechanism.

7. Third Party Data Access Requests

7.1 If Cloudflare becomes aware of any third party legal process requesting Personal Data that Cloudflare processes on behalf of Customer in its role as Processor or sub-Processor (as applicable) then Cloudflare will:

(a) immediately notify Customer of the request unless such notification is legally prohibited;

(b) inform the third party that it is a Processor or sub-Processor (as applicable) of the Personal Data and is not authorized to disclose the Personal Data without Customer's consent;

(c) disclose to the third party the minimum necessary Customer contact details to allow the third party to contact the Customer and instruct the third party to direct its data request to Customer; and

(d) to the extent Cloudflare provides access to or discloses Personal Data in response to third party legal process either with Customer authorization or due to a mandatory legal compulsion, then Cloudflare will disclose the minimum amount of Personal Data to the extent it is legally required to do so and in accordance with the applicable legal process.

7.2 In Cloudflare's role as a Processor or sub-Processor, as applicable, it may be subject to third party legal process issued by a government authority (including a judicial authority) and requesting access to or disclosure of Personal Data. If Cloudflare becomes aware of any third party legal process issued by a government authority (including a judicial authority) requesting Personal Data that Cloudflare processes on behalf of Customer in its role as Processor or sub-Processor (as applicable) then, to the extent that Cloudflare reviews the request with reasonable efforts and as a result is able to identify that such third party legal process requesting Personal Data raises a conflict of law, Cloudflare will:

(a) take all actions identified in clause 7.1 above;

(b) pursue legal remedies prior to producing Personal Data up to an appellate court level; and

(c) not disclose Personal Data until (and then only to the extent) required to do so under applicable procedural rules.

7.3 Clauses 7.1 and 7.2 shall not apply in the event that Cloudflare has a good-faith belief the government request is necessary due to an emergency involving the danger of death or serious physical injury to an individual. In such event, Cloudflare shall notify Customer of the data disclosure as soon as possible following the disclosure and provide Customer with full details of the same, unless such disclosure is legally prohibited.

7.4 Cloudflare will provide Customer with regular updates about third party legal process requesting Personal Data in the form of Cloudflare's semiannual Transparency Report, which is available at https://www.cloudflare.com/transparency/.

7.5 As of the date Customer entered into this DPA with Cloudflare, Cloudflare makes the commitments listed below. Cloudflare will update these commitments as may be required at https://www.cloudflare.com/transparency/:

(a) Cloudflare has never turned over our encryption or authentication keys or our customers' encryption or authentication keys to anyone.

(b) Cloudflare has never installed any law enforcement software or equipment anywhere on our network.

(c) Cloudflare has never provided any law enforcement organization a feed of our customers' content transiting our network.

(d) Cloudflare has never weakened, compromised, or subverted any of its encryption at the request of law enforcement or another third party.

8. General

8.1 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

8.2 Cloudflare's liability under or in connection with this DPA, including under the SCCs, is subject to the exclusions and limitations on liability contained in the Main Agreement. In no event does Cloudflare limit or exclude its liability towards data subjects or competent data protection authorities.

8.3 Except where and to the extent expressly provided in the SCCs or required as a matter of Applicable Data Protection Laws, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

8.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws as specified in the Main Agreement, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts specified in the Main Agreement.

8.5 If any provision of this DPA is, for any reason, held to be invalid or unenforceable, the other provisions of the DPA will remain enforceable. Without limiting the generality of the foregoing, Customer agrees that Section 8.2 (Limitation of Liability) will remain in effect notwithstanding the unenforceability of any provision of this DPA.

8.6 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter.

Annex 1

Data Processing Description

This Annex 1 forms part of the DPA and describes the processing that Cloudflare will perform on behalf of Customer.

A. LIST OF PARTIES

Data exporter(s): *Customer to complete the right-hand column.*

1.	Name: *Customer and any Customer Affiliates described in the Main Agreement.*	As stated in the Main Agreement
	Address: *Addresses of Customer and any Customer Affiliates described in the Main Agreement. (or otherwise notified by Customer to Cloudflare*	As stated in the Main Agreement
	Contact person's name, position and contact details:	As stated in the Main Agreement
	Activities relevant to the data transferred under this DPA and SCCs:	Use of the Service pursuant to the Main Agreement.
	Signature and date:	This Annex 1 shall be deemed executed upon execution of the DPA.
	Role (controller/processor):	Controller (or Processor on behalf of a third-party Controller).

Data importer(s):

1.	Name:	Cloudflare, Inc.
	Address:	101 Townsend Street San Francisco, CA 94107 USA
	Contact person's name, position and contact details:	Emily Hancock Data Protection Officer legal@cloudflare.com
	Activities relevant to the data transferred under this DPA and SCCs:	Processing necessary to provide the Service to Customer, pursuant to the Main Agreement.
	Signature and date:	This Annex 1 shall be deemed executed upon execution of the DPA.

	Role (Controller/Processor):	Processor (or sub-Processor)

B. DESCRIPTION OF DATA PROCESSING AND TRANSFER

Categories of data subjects whose Personal Data is transferred:	Natural persons that (i) access or use Customer's domains, networks, websites, application programming interfaces ("APIs"), and applications, or (ii) Customers' employees, agents, or contractors who access or use the Services, such as Cloudflare Zero Trust end users, (together, "End Users"). Natural persons with login credentials for a Cloudflare account and/or those who administer any of the Services for a Customer ("Administrators").
Categories of Personal Data transferred:	In relation to End Users: ● Any Personal Data processed in Customer Logs, such as IP addresses, and in the case of Cloudflare Zero Trust, Cloudflare Zero Trust end user names and email addresses. "Customer Logs" means any logs of End Users' interactions with Customer's Internet Properties and the Service that are made available to Customer via the Service dashboard or other online interface during the Term by Cloudflare. ● Any Personal Data processed in Customer Content, the extent of which is determined and controlled by the Customer in its sole discretion. "Customer Content" means any files, software, scripts, multimedia images, graphics, audio, video, text, data, or other objects originating or transmitted from or processed by any Internet Properties owned, controlled or operated by Customer or uploaded by Customer through the Service, and routed to, passed through, processed and/or cached on or within, Cloudflare's network or otherwise transmitted or routed using the Service by Customer. In relation to Administrative Users: ● Any Personal Data processed in Administrative User audit logs, such as IP addresses and email addresses.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Customer, its End Users, Administrators, and/or other partners may upload content to Customer's online properties which may include special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life. Any such special categories of data shall be protected by applying the security measures described in Annex 2.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous for the duration of the Main Agreement.
Nature of the processing:	Processing necessary to provide the Service to Customer, pursuant to the Main Agreement.
Purpose(s) of the data transfer and further processing:	Processing necessary for the provision of the Service.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable).
For transfers to (sub-) Processors, also specify subject matter, nature and duration of the processing:	The subject matter, nature and duration of the processing shall be as specified in the Main Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 of the SCCs)	In respect of the EU SCCs, means the competent supervisory authority determined in accordance with Clause 13 of the EU SCCs. In respect of the UK SCCs, means the UK Information Commissioner's Office.

Annex 2

Technical and Organisational Security Measures

Cloudflare has implemented and shall maintain an information security program in accordance with ISO/IEC 27000 standards. Cloudflare's security program shall include:

Measures of encryption of Personal Data

Cloudflare implements encryption to adequately protect Personal Data using:

- state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- trustworthy public-key certification authorities and infrastructure;
- effective encryption algorithms and parameterization, such as a minimum of 128-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Cloudflare enhances the security of processing systems and services in production environments by:

- employing a code review process to increase the security of the code used to provide the Services; and testing code and systems for vulnerabilities before and during use;
- maintaining an external bug bounty program;
- using checks to validate the integrity of encrypted data, and
- employing preventative and reactive intrusion detection.

Cloudflare deploys high-availability systems across geographically-distributed data centers.

Cloudflare implements input control measures to protect and maintain the confidentiality of Personal Data including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authenticating authorized personnel using unique authentication credentials (passwords) and hard tokens;
- automatically signing-out user IDs after a period of inactivity;
- protecting the input of data, as well as the reading, alteration and deletion of stored data; and
- requiring that data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked and secure.

Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

Cloudflare implements measures to ensure that Personal Data is protected from accidental destruction or loss, including by maintaining:

- disaster-recovery and business continuity plans and procedures;
- geographically-distributed data centres;
- redundant infrastructure, including power supplies and internet connectivity;
- backups stored at alternative sites and available for restore in case of failure of primary systems; and
- incident management procedures that are regularly tested.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Cloudflare's technical and organisational measures are regularly tested and evaluated by external third-party auditors as part of Cloudflare's Security & Privacy Compliance Program. These may include annual ISO/IEC 27001 audits; AICPA SOC 2 Type II; PCI DSS Level 1; and other external audits. Measures are also regularly tested by internal audits, as well as annual and targeted risk assessments.

Measures for user identification and authorisation

Cloudflare implements effective measures for user authentication and privilege management by:

- applying a mandatory access control and authentication policy;
- applying a zero-trust model of identification and authorisation;
- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- allocating and managing appropriate privileges according to role, approvals, and exception management; and
- applying the principle of least privilege access.

Measures for the protection of data during transmission

Cloudflare implements effective measures to protect Personal Data from being read, copied, altered or deleted by unauthorized parties during transmission, including by:

- using state-of-the-art transport encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- using trustworthy public-key certification authorities and infrastructure;
- implementing protective measures against active and passive attacks on the sending and receiving systems providing transport encryption, such as adequate firewalls, mutual TLS encryption, API authentication, and encryption to protect the gateways and pipelines through which data travels, as well as testing for software vulnerabilities and possible backdoors;
- employing effective encryption algorithms and parameterization, such as a minimum of 128-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms;
- using correctly implemented and properly maintained software, covered under a vulnerability management program, and tested for conformity by auditing;
- enforcing secure measures to reliably generate, manage, store and protect encryption keys; and
- audit logging, monitoring, and tracking data transmissions.

Measures for the protection of data during storage

Cloudflare implements effective measures to protect Personal Data during storage, controlling and limiting access to data processing systems, and by:

- using state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- using trustworthy public-key certification authorities and infrastructure;
- testing systems storing data for software vulnerabilities and possible backdoors;
- employing effective encryption algorithms and parameterization, such as requiring all disks storing Personal Data to be encrypted with AES-XTS using a key length of 128-bits or longer.
- using correctly implemented and properly maintained software, covered under a vulnerability management program, and tested for conformity by auditing;

- enforcing secure measures to reliably generate, manage, store and protect encryption keys;
- identifying and authorizing systems and users with access to data processing systems;
- automatically signing-out users after a period of inactivity; and
- audit logging, monitoring, and tracking access to data processing and storage systems.

Cloudflare implements access controls to specific areas of data processing systems to ensure only authorized users are able to access the Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- applying a zero-trust model of user identification and authorisation;
- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- monitoring actions of those authorised to delete, add or modify Personal Data;
- release data only to authorized persons, including the allocation of differentiated access rights and roles; and
- controlling access to data, with controlled and documented destruction of data.

Measures for ensuring physical security of locations at which Personal Data are processed

Cloudflare maintains and implements effective physical access control policies and measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers, and related hardware) where the Personal Data are processed or used, including by:

- establishing secure areas;
- protecting and restricting access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to data centers where Personal Data are hosted are logged, monitored, and tracked; and
- data centers where Personal Data are hosted are secured by security alarm systems, and other appropriate security measures.

Measures for ensuring events logging

Cloudflare has implemented a logging and monitoring program to log, monitor and track access to personal data, including by system administrators and to ensure data is processed in accordance with instructions received. This is accomplished by various measures, including:

- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- applying a zero-trust model of user identification and authorisation;
- maintaining updated lists of system administrators' identification details;
- adopting measures to detect, assess, and respond to high-risk anomalies;
- keeping secure, accurate, and unmodified access logs to the processing infrastructure for twelve months; and
- testing the logging configuration, monitoring system, alerting and incident response process at least once annually.

Measures for ensuring system configuration, including default configuration

Cloudflare maintains configuration baselines for all systems supporting the production data processing environment, including third-party systems. Configuration baselines should align with industry best

practices such as the Center for Internet Security (CIS) Level 1 benchmarks. Automated mechanisms must be used to enforce baseline configurations on production systems, and to prevent unauthorized changes. Changes to baselines are limited to a small number of authorized Cloudflare personnel, and must follow change control processes. Changes must be auditable, and checked regularly to detect deviations from baseline configurations.

Cloudflare configures baselines for the information system using the principle of least privilege. By default, access configurations are set to "deny-all," and default passwords must be changed to meet Cloudflare's policies prior to device installation on the Cloudflare network, or immediately after software or operating system installation. Systems are configured to synchronize system time clocks based on International Atomic Time or Coordinated Universal Time (UTC), and access to modify time data is restricted to authorized personnel.

Measures for internal IT and IT security governance and management

Cloudflare maintains internal policies on the acceptable use of IT systems and general information security. Cloudflare requires all employees to undertake general security and privacy awareness training at least every year. Cloudflare restricts and protects the processing of Personal Data, and has documented and implemented:

- a formal Information Security Management System (ISMS) in order to protect the confidentiality, integrity, authenticity, and availability of Cloudflare's data and information systems, and to ensure the effectiveness of security controls over data and information systems that support operations; and
- a formal Privacy Information Management System (PIMS) in order to protect the confidentiality, integrity, authenticity, and availability of the policies and procedures supporting Cloudflare's global managed network, as both a processor and a controller of customer information.

Cloudflare will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Cloudflare shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Annex 2.

Measures for certification/assurance of processes and products

The implementation of Cloudflare's ISMS and related security risk management processes have been externally certified to the industry-standard ISO/IEC 27001. The implementation of Cloudflare's comprehensive PIMS has been externally certified to the industry-standard ISO/IEC 27701, as both a processor and controller of customer information.

Cloudflare maintains PCI DSS Level 1 compliance for which Cloudflare is audited annually by a third-party Qualified Security Assessor. Cloudflare has undertaken other certifications such as the AICPA SOC 2 Type II certification in accordance with the AICPA Trust Service Criteria, and details of these and other certifications that Cloudflare may undertake from time to time will be made available on Cloudflare's website.

For transfers to (sub-) Processors, also describe the specific technical and organisational measures to be taken by the (sub-) Processor to be able to provide assistance to the controller (and, for transfers from a Processor to a sub-Processor, to the data exporter).

Measure	Description
Self-service access to meet data subject rights of access, erasure, rectification etc.	Ability to login to review and edit Personal Data via the Cloudflare dashboard.