MOZILLA VENDOR DATA PROCESSING ADDENDUM

This Mozilla Vendor Data Processing Addendum ("**DPA**") supplements the Agreement (as defined below) entered into by and between Mozilla Corporation (together with any Affiliate of Mozilla Corporation, "**Mozilla**") and the entity, organization, or party identified in the applicable Agreement (the "**Vendor**").

The parties hereby enter into this DPA in order to comply with the obligations under Applicable Data Protection Laws (as defined below). Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. In the event of any conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall control to the extent of any such conflict or inconsistency.

1. Certain Definitions.

a. "**Affiliate**" means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with such party. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the applicable entity.

b. "**Agreement**" means any agreement between Mozilla and Vendor under which Vendor engages in the Processing of Mozilla Data in the course of providing such services.

c. "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, without limitation: (i) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**"), together with any applicable EU Member State laws implementing the GDPR; (ii) the UK Data Protection Act 2018, as amended, and the GDPR as incorporated into UK law as the UK GDPR, as amended ("**UK GDPR**"); (iii) the Swiss Federal Act of 19 June 1992 on Data Protection, as may be amended or superseded, and its implementing regulations ("**Swiss DPA**"); and (iv) the California Consumer Privacy Act of 2018 ("**CCPA**"), as amended by the California Privacy Rights Act of 2020 ("**CPRA**"), together with its implementing regulations.

d. "**Controller**" means the entity that determines the purposes and means of Processing of Mozilla Data.

e. "**Information Security Incident**" means any confirmed breach of security that leads to the accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Mozilla Data processed by Vendor and/or its Sub-processors in connection with the provision of the Services. For the avoidance of doubt, "Information Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of Mozilla Data,

including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

f. "**Mozilla Data**" means Personal Data that is Processed by Vendor in connection with Vendor's performance of the Services.

g. "**Mozilla End User**" means an identified or identifiable person or entity to which Mozilla Data relates, and may include, without limitation, Mozilla's users and customers, employees, contractors, suppliers, and other third parties.

h. "**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity that has standing and protection under Applicable Data Protection Laws.

i. "**Processing**" or "**Process**" or "**Processed**" shall refer to any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

j. "**Processor**" means the entity that Processes Mozilla Data.

k. "**Services**" shall mean any product or service provided or performed by Vendor pursuant to the Agreement.

l. "**Standard Contractual Clauses**" means the contractual clauses annexed to the European Commission Implementing Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

m. "**UK Addendum**" means the UK 'International Data Transfer Addendum to the EU Commission Standard Contractual Clauses' issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018.

2. Processing of Mozilla Data.

a. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Mozilla Data, Mozilla may either act as a Controller or Processor of Mozilla Data, and Vendor is the Processor acting on behalf of Mozilla.

b. **Processing Instructions**.

i. Vendor, in its capacity as a Processor on behalf of Mozilla, will Process Mozilla Data only as necessary to perform the Services and otherwise

comply with its obligations under the Agreement or Applicable Data Protection Laws, and shall only Process Mozilla Data in accordance with the documented, lawful instructions of Mozilla, as set forth in the Agreement, in this DPA, or as may otherwise be directed by Mozilla in accordance with Applicable Data Protection Laws (the "**Permitted Purpose**").

ii. Vendor will not retain, use, disclose, or otherwise Process the Mozilla Data outside of the direct business relationship between Mozilla and Vendor.

iii. Vendor will not use, disclose, or otherwise Process the Mozilla Data for any purpose other than the Permitted Purpose, and will not sell, rent, or lease Mozilla Data within the meaning of Applicable Data Protection Laws.

iv. Vendor will promptly inform Mozilla if Vendor becomes aware that Mozilla's instructions for Processing of Mozilla Data infringe or otherwise violate Applicable Data Protection Laws.

v. As between Mozilla and Vendor, Mozilla shall have sole responsibility for the accuracy, quality, and legality of Mozilla Data and the means by which Mozilla acquired Mozilla Data. Vendor acknowledges that, as between Mozilla and Vendor, Mozilla (or the applicable Mozilla End User) owns all right, title, and interest in and to the Mozilla Data.

c. Details of the Processing of Mozilla Data.

i. The subject matter of the Processing of Mozilla Data by Vendor is the performance of the Services pursuant to the Agreement.

ii. The duration of the Processing of Mozilla Data is as set forth in the Agreement.

iii. The purpose of the Processing of Mozilla Data is the provision of the Services by Vendor to Mozilla as set forth in the Agreement.

iv. The nature of the Processing of Mozilla data is the provision of the Services and the fulfillment of contractual obligations to Mozilla, as set forth in the Agreement. These Services may include the Processing of Mozilla Data by Vendor.

v. Categories of Data Subjects: Mozilla determines the data subjects, which may include Mozilla End Users.

vi. Categories of Data: Mozilla determines the categories of Personal Data, including Mozilla Data, that it submits to the Services.

3. **Sub-Processing of Mozilla Data**. Vendor may, with prior written permission from Mozilla, transfer Mozilla Data to third-party Processors ("**Subprocessors**") for the limited purpose of providing the Services. Where Vendor subcontracts duties that require third-party Processing of Mozilla Data, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Vendor under this DPA with respect to the Processing of Mozilla Data. Mozilla may request from the Vendor a current list of Vendor's Subprocessor at any time. Vendor shall notify Mozilla in writing at least thirty (30) days before authorizing any new Subprocessor that will Process Mozilla Data. Mozilla may reasonably object to Vendor's use of any new Subprocessor within this thirty (30) day period. If Mozilla objects to any new Subprocessor, the parties will work in good faith to resolve the matter, including Vendor making commercially reasonable efforts to (i) find a substitute Subprocessor that is acceptable to Mozilla or (ii) continuing to provide the same level of Services without the Subprocessor. If the parties cannot resolve the matter within thirty (30) days of Mozilla's notification of objection, Mozilla may terminate the Agreement immediately without penalty and Vendor will return to Mozilla any prepaid fees unearned as of the date of Mozilla's notification of termination. Vendor shall be liable for any and all acts and omissions of its Subprocessor to the same extent Vendor would be liable if performing the services of any Subprocessor directly under the terms of this DPA.

4. **Vendor Obligations**.

a. **Confidentiality**.

i. Vendor will maintain as confidential and will not disclose Mozilla Data to any third party (including for back-up purposes), except as expressly permitted by this DPA or as required by law.

ii. Vendor will take appropriate steps to ensure that its employees, authorized agents, and any authorized Subprocessors are informed of the confidential nature of the Mozilla Data, have agreed in writing to maintain such Mozilla Data as confidential (including after the termination of their employment, contract, or assignment) and have received appropriate training on their responsibilities in respect of Mozilla Data Processing. Vendor shall ensure the reliability of its personnel engaged in the Processing of Mozilla Data and shall ensure that access thereto is limited to personnel performing Services in connection with the Agreement.

iii. Vendor may disclose Mozilla Data under a valid order of a court or other governmental body, but only to the extent and for the purposes of such order; provided that, if legally permissible Vendor agrees to inform Mozilla in writing of the request, give Mozilla the opportunity to defend against the order, and limit its disclosure to only the information legally required to be disclosed.

b. **Security Measures**. Vendor shall adopt and maintain appropriate organizational, technical and security measures, including those described in Exhibit B attached hereto, prior to the commencement of the Processing of Mozilla Data. Vendor will, at a minimum, maintain such measures for the duration of the Agreement, and will provide Mozilla with reasonable evidence of its privacy and security policies.

c. **Aggregation of Mozilla Data**. Except solely to provide Mozilla with the Services and except in a manner disclosed to and authorized in writing by Mozilla, Vendor shall not correlate or aggregate any Mozilla Data with any other data obtained through other products, services, web properties or from third parties in any way that could (i) identify an individual, a specific device, Mozilla, or its parents or subsidiaries or (ii) to expand existing or create new profiles about Mozilla or any individuals.

5. Information Security Incidents.

a. If Vendor deliberately or inadvertently Processes Mozilla Data in breach of this DPA or Vendor discovers, is notified of, or has reasonable awareness that an Information Security Incident is likely to occur, Vendor shall immediately notify the Mozilla project contact, as well as compliance@mozilla.com, describing the nature of the Information Security Incident (or anticipated Information Security Incident) and the Mozilla Data implicated (or likely to be implicated).

b. In the event of an Information Security Incident, Vendor shall investigate, remediate, and mitigate the effects of the Information Security Incident, and shall provide Mozilla with assurances satisfactory to Mozilla that such Information Security Incident has been resolved and will not recur.

6. Data Subject Rights; Cooperation.

a. Taking into account the nature of the Processing, Vendor must provide reasonable and timely assistance to Mozilla (at Mozilla's expense) to enable Mozilla to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Laws (including the rights of access, to rectification, to erasure, to restriction, to objection, and data portability, as applicable); and (ii) any other correspondence, inquiry, or complaint received from a data subject, regulator or other third party, in each case in respect of Mozilla Data that Vendor Processes on behalf of Mozilla ((i) and (ii) each being a "**Data Subject Request**").

b. In the event any Data Subject Request is made directly to Vendor in its capacity as a Processor hereunder, Vendor will not respond to such Data Subject Request directly without Mozilla's prior authorization, unless legally required to do so. If Vendor is legally required to respond to a Data Subject Request, Vendor will promptly notify Mozilla and provide it with a copy of the Data Subject Request (unless legally prohibited from doing so).

c. Vendor will, at Mozilla's request and expense, provide reasonable information, assistance, and cooperation regarding the Services (and/or Vendor's Processing) to enable Mozilla to carry out data protection impact assessments or prior consultations with data protection authorities, if applicable.

7. Audit. Vendor agrees, upon reasonable prior request by Mozilla, to submit its facilities, records, systems, staff, subcontractors, and practices, together with any other data, deemed by Mozilla to be relevant to Vendor's Processing of Mozilla Data, to reasonable review and audit to ensure compliance with Applicable Data Protection Laws (or any other law or regulation) and the terms and conditions of this DPA. Any such review or audit shall be carried out by Mozilla (or an agent of Mozilla bound by a duty of confidentiality), at Mozilla's expense.

8. Deletion or Return of Mozilla Data. Upon termination of the Agreement, or upon written request from Mozilla, Vendor will cease all Processing of Mozilla Data, and will delete or return (at Mozilla's choice) to Mozilla all Mozilla Data (including copies) Processed on behalf of Mozilla in connection with the Agreement. To the extent Vendor is required under applicable law to retain some or all of the Mozilla Data, Vendor will do so only to the extent and for the duration necessary to comply with applicable law, will continue to retain such Mozilla Data in compliance with the requirements of this DPA, and will protect the Mozilla Data from further Processing.

9. International Data Transfers.

a. Mozilla and Vendor agree that the Standard Contractual Clauses shall apply only to Processing by Vendor of Mozilla Data that involves a transfer from the European Economic Area, the United Kingdom, or Switzerland to a jurisdiction that does not ensure an adequate level of protection for Personal Data (a "**Restricted Transfer**"). The Standard Contractual Clauses are attached hereto as Exhibit A and are hereby incorporated by reference. If Vendor's Processing involves a Restricted Transfer of Mozilla Data, Vendor hereby agrees that it shall only conduct such Processing as described in the Standard Contractual Clauses.

b. For Restricted Transfers of Mozilla Data protected under the UK GDPR, the UK Addendum shall be deemed executed between Mozilla and Vendor, and the Standard Contractual Clauses shall be deemed amended as specified by the UK Addendum. The Tables of the UK Addendum shall be deemed completed with the information as set forth in Exhibit 3.

c. For Restricted Transfers of Mozilla Data protected under the Swiss DPA, the Standard Contractual Clauses shall be modified as follows:

(i) references to "Directive 95/46/EC" or "Regulation EU2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to 'Regulation (EU) 2018/1725" are removed;

(iii) references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as applicable;

(iv) references to the "competent supervisory authority" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner;

(v) references to the 'competent courts' shall be interpreted as references to the competent courts in Switzerland;

(vi) Clause 17 shall be replaced with the following: "These Clauses shall be governed by the law of Switzerland."; and

(vii) Clause 18(a) and 18(b) shall be replaced with the following: "Any dispute arising from these Clauses shall be resolved by the courts of Switzerland."

10. Notices. Any notice required to be given to Mozilla under this DPA shall be provided to Mozilla at legal-notices@mozilla.com, with a copy to compliance@mozilla.com.

11. Relationship with Agreement. Mozilla and Vendor agree that this DPA replaces and supersedes any existing or previously entered DPA between the parties in connection with the Services. In the event of any conflict between this DPA and the Agreement, the terms of this DPA shall control. In the event of a conflict or inconsistency between the terms set forth in the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

EXHIBIT A: 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 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 (Docking clause) – Omitted

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

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Exhibit B and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her

rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Exhibit B. 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 within twenty-four (24) hours 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) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 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 Exhibit B 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) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

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

STANDARD CONTRACTUAL CLAUSES - APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Mozilla Corporation

Name: Mozilla Corporation

Address: 149 New Montgomery Street, Fourth Floor, San Francisco, CA 94105

Contact person's name, position and contact details: Mozilla Compliance (compliance@mozilla.com)

Activities relevant to the data transferred under these Clauses: To receive the Services and otherwise perform its obligations under the Agreement

Signature and date: Data exporter's signature to the Agreement shall constitute Data exporter's signature of the standard contractual clauses

Role (controller/processor): Controller

Data importer(s):

1. Name: As set forth on the first page of the Agreement

Address: As set forth on the first page of the Agreement

Contact person's name, position and contact details: As set forth on the first page of the Agreement

Activities relevant to the data transferred under these Clauses: To provide the Services and otherwise perform its obligations under the Agreement.

Signature and date: Data importer's signature to the Agreement shall constitute Data importer's signature of the standard contractual clauses

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described in the Agreement, the Addendum, and/or the applicable Statement of Work

Categories of personal data transferred

As described in the Agreement, the Addendum, and/or the applicable Statement of Work

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.

N/A, unless otherwise described in the Agreement and/or the applicable Statement of Work

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

As described in the Agreement and/or the applicable Statement of Work

Nature of the processing

As described in the Agreement, the Addendum, and/or the applicable Statement of Work

Purpose(s) of the data transfer and further processing

As described in the Agreement, the Addendum, and/or the applicable Statement of Work

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

The period for which the personal data will be retained shall be for as long as Vendor provides Services to Mozilla and thereafter as permitted by the Agreement and/or the Addendum.

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

As necessary for Vendor to provide the Services, and in accordance with the Addendum

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

To be determined in accordance with Clause 13 of the Standard Contractual Clauses.

EXHIBIT B: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures must include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- Multi-factor support for authentication processes
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

3. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised input, reading, copying, removal modification or disclosure of data. These measures must include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems
- Measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment

4. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures must include:

- Encryption for remote access, transport and communication of data

- Prohibition of portable media
- Creating an audit trail of all data transfers

5. **Input control**

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained. Measures must include:

- Logging user activities on IT systems
- Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input

6. **Job control**

Measures must be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

7. **Availability control**

Measures must be put in place to ensure that data are protected against accidental destruction or loss. These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Protect stored personal data against data corruption, and ensure ability to identify and restore corrupted data
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Firewall and intrusion detection systems

8. **Segregation control**

Measures must be put in place to allow data collected for different purposes to be processed separately. These must include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

Exhibit 3

UK Addendum to the Standard Contractual Clauses

TABLE 1	
PARTIES	The Parties are set out in Annex I of the Standard Contractual Clauses attached to this DPA as Exhibit A
TABLE 2	
SELECTED SCCS, MODULES AND SELECTED CLAUSES	The version of the Standard Contractual Clauses attached to this DPA as Exhibit A
TABLE 3	
APPENDIX INFORMATION	Annex 1A: List of Parties: As set forth for the data exporter and data importer in Annex I (Section A) of the Standard Contractual Clauses attached to this DPA as Exhibit A
	Annex 1B: Description of Transfer: As set forth in Annex I (Section B) of the Standard Contractual Clauses attached to this DPA as Exhibit A
	Annex II: As set forth in Exhibit B of this DPA
	Annex III: As set forth in Annex 1 (Section B) of the Standard Contractual Clauses attached to this DPA as Exhibit A
TABLE 4	
ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES	The data exporter shall have the right to end this Approved Addendum pursuant to Section 19 of the UK Addendum.