DATA PROCESSING Addendum

Addendum to the Disqus Publisher Terms of Service Agreement

This Addendum to the Disqus Publisher Terms of Service Agreement (the "DPA Addendum" or "DPA"), effective as of the Effective Date as set forth on the Agreement, specifies the global data protection obligations of Disqus Inc. ("Disqus") and publisher ("Publisher") under any agreement by which Disqus and Publisher process Personal Data and forms part of the Disqus Publisher Terms of Service Agreement ("Agreement") previously entered into by the parties hereto.

WHEREAS, Disqus provides Publisher with the Disqus commenting application service (the "Disqus Comments" or "Services") through which Disqus collects certain Personal Data from website users visiting the Publisher's websites where the Disqus Comments are loaded, and Disqus further provides Publisher with the ability to access the comments left users on their website as well as some of the Personal Data associated with such comments;

WHEREAS, Privacy and Data Protection Laws (as defined below) impose compliance obligations upon Disqus and Publisher in relation to the collection and processing of Personal Data.

NOW THEREFORE, Pursuant to the requirements of the Privacy and Data Protection Laws , Disqus and Publisher hereby enter into this DPA.

Definitions

1.1 For the purposes of this DPA:

(a) **"EEA"** means the member states of the European Union and Iceland, Liechtenstein, Norway and the United Kingdom.

(b) **"Controller" or "Co-Controller"** shall mean an entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;

(c) **"Processor"** shall mean an entity which processes Personal Data on behalf of the Controller;

(d) **"Personal Data"** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, and identification number, location data or online identifier.

(e) **"Disqus Personal Data"** means comments, content, data and information that is displayed, uploaded, exchanged, transmitted or collected through the Services provided to Publisher.

(f) **"Publisher Personal Data"** means all Personal Data provided by or collected on behalf of Publisher like single sign on data under the Agreement.

(g) "**Business Purpose**" means the purpose of providing the Services or any other purpose specifically identified in Exhibit A.

(h) "**Process**" **or "Processing"** means any operation or set of operations performed upon Personal Data, whether or not by automatic means

(i) "**Standard Contractual Clauses**" or **"SCC"** means the applicable module(s) of the European Commission's 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, as set out in the Annex to Commission Implementing Decision (EU) 2021/914, a completed copy of which comprises Exhibit B.

(j) **"Restricted Country"** means a member state of the European Economic Area, Argentina, Brazil, China, Costa Rica, Ghana, Hong Kong, Israel, Malaysia, Mexico, Morocco, Russia, Singapore, Switzerland, Tunisia, Turkey, the United Kingdom, or Uruguay.

2. Applicability of DPA.

2.1. This DPA will apply to the extent that Publisher and Disqus Process Disqus Personal Data as Co-Controllers. To the extent that Publisher transfers Publisher Personal Data to Disqus, Disqus shall be a Processor and Publisher shall be a Controller.

2.2 This DPA is subject to the terms of the Agreement and is incorporated into the Agreement. Interpretations and defined terms set forth in the Agreement apply to the interpretation of this DPA.

2.3 The Appendices form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Appendices.

3. Roles and responsibilities.

3.1 Parties' Roles.

Co-Controller. Disqus and Publisher each act as a Co- Controller with respect to the Disqus Personal Data processed hereunder. EXHIBIT A describes the Personal Data that Disqus makes available to Publisher and the purposes therefor. Publisher and Disqus undertake to access and use the Personal Data provided by Disqus only to the extent reasonably necessary to achieve the purposes of the processing.

Publisher as Controller and Disqus as Processor. To the extent that Publisher transfers Publisher Personal Data to Disqus, Publisher shall be the Controller of Publisher Personal Data, and Disqus shall be the Processor and Process Publisher Personal Data only in accordance with the permitted purposes.

3.2 Purpose Limitation. Both parties shall process the Personal Data solely for the purposes described in EXHIBIT A, except where required by applicable law.

3.3 Compliance: Each party, as Controller and Disqus as Processor, where applicable, shall be responsible for ensuring that it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including but not limited to the EU data protection legislation ("Privacy and Data Protection Laws").

3.4 Representations and warranties. Each party represents and warrants that it has sufficient legal rights to and in any Personal Data in order to transmit it to the other party as set forth herein or in the Agreement.

3.5 CPRA. Both parties, for the purposes of this DPA, may be deemed under the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 ("CPRA") to share Personal Data to the other party. Both parties agree to comply with the requirements set forth in the CPRA Addendum described in Exhibit C.

3.5 Written authorization. Each party will only Process Personal Data pursuant to written directions as specified in the Agreement.

3.6 Publisher's rights and responsibilities. Publisher has the technical means to turn off the collection and sharing of Personal Data by the Services at any time. Publisher is responsible for all content moderation which includes

approval or removal of comments, blocking of users, setting up keyword alerts for content violation, and editing keywords.

3.7 Accuracy. Both parties shall ensure that Personal Data is accurate and, where necessary kept up to date, relevant, adequate, and in compliance with all applicable privacy and data security laws, rules and regulations.

4. Security

4.1 Security. Publisher and Disqus shall implement appropriate technical and organizational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (each a "Security Incident"). Disqus will allow and cooperate with Publisher to conduct reasonable assessments or Disqus may arrange for a qualified and independent assessor to conduct an assessment of Disqus' policies and technical and organizational measures, at least annually and at Disqus' expense. Disqus shall provide a report of such assessment to Publisher upon request.

4.2 Confidentiality of Processing. Publisher and Disqus shall ensure that any person that it authorizes to process the Personal Data shall be subject to a contractual or statutory duty of confidentiality. Neither party shall sell, rent, lease, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Personal Data to another business, person, or third party without the other party's prior written consent.

4.3 Security Incidents. Each party will promptly and without undue delay and in any case no later than twenty-four (24) hours of becoming aware, inform the other party in the event of: (i) any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosures of, or access to, Personal Data (altogether, a "**Security Incident**"), or (ii) any reasonable suspicion of a Security Incident, regardless of its cause. At Co-Controller's direction, Controller will provide all relevant information and assistance required by Co-Controller to investigate, mitigate and respond to a Security Incident, including at a minimum, any information or assistance required by applicable Privacy and Data Protection Laws.

4.4 Requests from data protection authorities. Co-Controller shall reasonably assist Controller in response to any requests from data protection authorities relating to the Processing of Personal Data in connection with the Agreement. In the event that any such request is made directly to Co-Controller, Controller shall not respond to such communication directly without Co-Controller's prior authorization, unless legally compelled to do so. If Controller is required to respond to such a request, Controller shall promptly notify Co-Controller and provide it with a copy of the request unless legally prohibited from doing so.

5. Sub-processing

5.1 Processors and sub-Processors. Co-Controller may engage Co-Controller affiliates and third party Data Processors or sub-Processors to process the Personal Data. Co-Controller shall inform Controller of any intended changes concerning the addition or replacement of sub-Processors, giving Controller the opportunity to object to such changes. Co-Controller shall impose on such Processors data protection terms that protect the Personal Data to the same standard provided for by this DPA and shall remain liable for any breach of the DPA caused by a Processor or sub-Processor. If Co-Controller subcontracts or assigns any of Co-Controller's obligations to a third party, Co-Controller will in each case: (a) first ensure that each and every such subcontractor, partner or assignee (as the case may be) has undertaken in signed writing to comply with obligations no less protective than the obligations undertaken by Co-Controller in this Addendum; (b) perform appropriate due diligence to ensure that all subcontractors, partners and assignees can meet all Co-Controller obligations in the Agreement, including all requirements related to features, functionality and assistance necessary for data subject requests; (c) remain fully liable for the performance of each subcontractor, partner and/or assignee; and (d) enter into Standard Contractual Clauses.

6. International transfers.

6.1 International Transfers:

Where Co-Controller transfers Personal Data outside the EEA in a country in respect of which a valid adequacy decision has not been issued by the European Commission or adequacy has not otherwise been determined in another valid method under applicable data protection laws then an adequate level of protection shall be put in place by entering into Standard Contractual Clauses, a completed copy of which comprises Exhibit B and which are hereby incorporated by reference or through any other recognized methods. Co-Controller authorizes any transfers of Personal Data to, or access to Personal Data from, such destinations outside the EEA subject to such adequacy measures having been taken. The Controller-to-Processor Standard Contractual Clauses shall apply in all cases where Personal Data that relates to residents of the EEA is Processed by Disqus. The Controller-to-Controller Standard Contractual Clauses will also apply where, and to the extent that, Publisher acts as a Co-Controller with respect to any Personal Data that relates to a resident of the EEA. In particular, and without limiting the above obligations:

i. Publisher and Disqus agree that their respective obligations under the Standard Contractual Clauses shall be governed by the law(s) of the Member State(s) (or Switzerland or the United Kingdom) in which Publishers are established; and
ii. the details of the appendices applicable to the Standard Contractual Clauses are set out in **Exhibit B** to this Addendum.

6.2 Disclosure to authorities: Co-Controller acknowledges that Controller may disclose the privacy provisions in this DPA and the Agreement to the US Department of Commerce, the Federal Trade Commission, a European data protection authority, or any other US or EU judicial or regulatory body upon their lawful request.

7. Cooperation

7.1 Cooperation and data subjects' rights. Co-Controller shall reasonably cooperate with Controller in all matters pertaining to the Personal Data and shall provide Controller information about its uses of Personal Data upon request. Co-Controller shall respond and give effect to requests from data subjects seeking to exercise their rights under Privacy and Data Protection Laws. If Co-Controller cannot reasonably respond to a request by a data subject it may refer the data subject to Controller as appropriate. Co-Controller will provide all other reasonable assistance and execute such agreements as may be necessary to legitimize any Processing or data transfer of Personal Data to Controller or a subcontractor and to ensure an adequate level of protection for Personal Data. In the event that any competent authority holds that a data transfer mechanism relied on by the parties is invalid, or any supervisory authority requires transfers of Personal Data made pursuant to such decision to be suspended, then Co-Controller may, at its discretion, require Controller to cease Processing Personal Data, or co-operate with it to facilitate use of an alternative transfermechanism.

7.2 Data Protection Impact Assessments: Co-Controller shall, to the extent required by Privacy and Data Protection Laws, provide Controller with commercially reasonable assistance with any future data protection impact assessments or prior consultations with data protection authorities that Controller is required to carry out under Privacy and Data Protection Laws.

8. Security reports and audits.

8.1 Co-Controller shall provide, upon Controller's request, copies of any relevant summaries of external security certifications or security audit reports necessary to verify Publisher’s compliance with this DPA.

8.2 While it is the parties' intention ordinarily to rely on the provision of the documentation at 8.1 above to verify Co-Controller's compliance with this DPA, Co-Controller shall permit Controller (or its appointed third party auditors) to carry out an audit of Co-Controller's Processing of Personal Data under the Agreement following a Security Incident suffered by Controller, or upon the instruction of a data protection authority. Controller must give Co-Controller reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Co-Controller's operations. Any such audit shall be subject to Co-Controller's security and confidentiality terms and guidelines.

8.3 Each Controller shall implement reasonable and appropriate technical, physical, and organizational measures designed to adequately safeguard and protect against a Security Incident (each, a "**Security Measure**"). Such Security Measures shall require each Controller to have regard to industry standards and costs of implementation as well as taking into account the nature, scope, context, and purposes of the Processing as well as the risk of harm that may result from a Security Incident to Co-Controller.

9. Deletion or return of data: Upon termination or expiry of the Agreement, each Controller shall delete the Personal Data (including copies) then in Controller's possession, except to the extent that Controller is required by an applicable law to retain some or all of the Personal Data.

10. Term: The term of this Addendum commences as of the Addendum Effective Date and will end upon the termination of the Agreement. However, each Controller's obligations hereunder continue in effect until any Personal Data subject to this DPA is returned or destroyed

11. Indemnity: Any indemnity obligations will be covered pursuant to the Agreement.

12. Governing Law: Unless otherwise required by the Standard Contractual Clauses or other data transfer requirements, this Addendum will be subject to the governing law identified in the Agreement without giving effect to conflict of laws principles.

13. Counterparts: This Addendum may be entered into by the parties in any number of counterparts. Each counterpart will, when executed and delivered, be regarded as an original, and all the counterparts will together constitute one and the same instrument.

14. Modifications: During the term of this DPA, Disqus may revise the terms and conditions of this DPA at any time. Any such revision or change will be binding and effective immediately on posting of the revised DPA on Disqus' homepage.

IN WITNESS WHEREOF, Disqus and Publisher have executed this Addendum, effective as of the date the Agreement is signed (the "**Addendum Effective Date**").

IN WITNESS WHEREOF the parties hereto have executed this Addendum as of the date first mentioned above:

Acknowledged and Agreed to:

Disqus, Inc.	PUBLISHER:
Signed: 	Signed: _____
Name: Steven Stein	Name: _____
Title: President, Disqus	Title: _____
Date: _____	Date: _____

EXHIBIT A DETAILS OF THE PROCESSING

Description of Disqus: Disqus, Inc. is the legal entity that has executed the Agreement with Publisher for the provision of Disqus' commenting application services on Publisher's website.

Purposes of Processing: Disqus provides a commenting application service ("Disqus Comments") to Publisher for use as a comment forum on the Publisher's website. Disqus collects Personal Data from users commenting in the Disqus Comments on Publisher's website. Disqus provides Publisher with access to the comments so that Publisher may act as moderator on its website, and to meet its relevant obligations under applicable laws. The comments may include Personal Data such as email address, username, IP address or other online identifier, which Publisher may process solely for the purpose of moderating Publishers' site(s).

Type(s) of Personal Data Processed: Email address, username, IP address, other online identifier, information revealed in user comments.

Special categories of data (if applicable): Disqus does not intentionally collect, and Publisher does not intentionally transfer any sensitive personal data in relation to these data subjects. Publisher may collect categories of sensitive personal data contained in user comments as part of its comment moderation activities only in accordance with applicable privacy laws.

Categories of Data Subjects: The Personal Data Processed concern individuals who access the Publishers website on which the Disqus Comments are loaded.

Nature of Processing Operations: Publisher will Process the Personal Data solely for the purpose of moderating the comments on their website and meeting any applicable legal requirements.

Duration of the Processing: As set forth in the Agreement.

EXHIBIT B STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES

Controller to Controller

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 8.5 (e) and Clause 8.9(b);

(iii) N/A

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

(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**

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8: **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance

with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they 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 subject. 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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data 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') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9: **Use of sub-processors** N/A

Clause 10: **Data subject rights**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or 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 _____ (*specify Member State*).

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 _____ (*specify Member State*).

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses: Use of the Disqus Commenting Platform

Signature and date: _____

Role (controller/processor): Co-Controller

Data importer(s):

Name: Disqus, Inc.

Address: 3 Park Avenue, 33rd Floor, New York, NY 10016

Contact person's name, position and contact details: Steven Stein, steven.stein@disqus.com

Activities relevant to the data transferred under these Clauses: Providing the Disqus Commenting Platform.

Signature and date: _____

Role (controller/processor): Co-Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users that use the Disqus comment function on a publisher's website

Categories of personal data transferred

Email addresses, username, IP address, other online identifier, information revealed in user comments.

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.

NA

The frequency of the transfer

Depends on user's use of the Disqus comment function

Nature of the processing

Disqus provides a commenting application service ("Disqus Comments") to publisher for use as a comment forum on the publisher's website. Disqus collects personal data from users commenting in the Disqus Comments on publisher's website. Disqus provides publisher with access to the comments so that publisher may act as moderator on its website, and to meet its relevant obligations under applicable laws.

Purpose(s) of the data transfer and further processing

To fulfil user's request to comment on publisher's website.

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

To fulfil the purposes of processing personal data.

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

C. COMPETENT SUPERVISORY AUTHORITY

ANNEX II

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

A. Technical Measures

1. Information Security Policy

1.1. Disqus maintains a written information security policy which shall include, at a minimum, the approach adopted by Disqus to address the confidentiality, integrity, and availability of Disqus, its affiliates' and representatives', and its customers' confidential information, as applicable, which at least meets the minimum standards of (a) International Standard ISO.IEC 27001 and 27002 or (b) a similar industry-standard framework.

2. Testing and Scanning Procedures

2.1. Penetration testing: Upon request, Disqus provides Publisher with an executive summary of the results of penetration testing.

2.2. Information security certification: Upon request, Disqus provides Publisher with a third-party information security certification such as ISO 27K and SOC 2 Type II from an industry-recognized third party as of such then-completed year.

2.3. Vulnerability scanning: Upon request, Disqus provides Publisher with executive summaries of external, internal, and web application vulnerability scanning. If Publisher identifies elevated risks present within provided information, Disqus will promptly remediate identified risks at Disqus' expense. Disqus adheres to OWASP coding principles for web application code and uses static or dynamic application vulnerability scanning or manual code review, when appropriate. Disqus ensures that vulnerability scans periodically are conducted on devices and software present in its internal and external network environments and web applications to identify and remediate or have remediated any vulnerabilities within a documented timeframe. Disqus will provide Publisher with summaries of such scans and results upon request.

2.4. Penetration tests: Disqus conducts annual penetration tests on all its externally facing critical systems and applications from an industry-recognized independent third party at Disqus 'expense. Disqus conducts similar such tests after significant changes are made to its network. Such penetration tests shall:

(a) be based on industry-accepted penetration testing approaches (e.g. NIST SP800-115),
(b) include testing from inside and outside the network,
(c) include testing to validate segmentation, and
(d) include network-layer, operating system, and application layer testing such that, at a minimum, they test against vulnerabilities identified in industry standards (e.g. OWASP Guide, SANS CWE Top 25, CERT Secure Coding).

3. Backups

Disqus maintains secure, usable, and traceable data/information backups to ensure that backups can be used when necessary.

4. Internal Hardware Protection

4.1. Disqus ensures that all computing and storage devices on its network, including but not limited to, workstations, servers, and network devices have endpoint protection in place consistent with industry standards, such as anti-malware, email, and application scanning, or antivirus.

4.2. Disqus has a tiered network architecture, which includes preventive and detective devices and where highly sensitive non-public information is in a secured and segregated network.

4.3. Disqus ensures that the network devices, servers, and workstations where Publisher information is located are hardened and continuously subject to minimum security baselines.

4.4. Disqus maintains an inventory of authorized devices that can be connected to its network environment and ensures that such inventory is reconciled periodically.

4.5. Disqus maintains an inventory of authorized software required for its network devices, servers, and workstations present in its network environment and ensures that such inventory is reconciled periodically.

4.6. Disqus maintains a change management methodology that ensures only approved changes are released and deployed in the production environment.

4.7. Disqus conducts periodic reviews of its cloud computing use based on the cloud security alliance risks and controls structure and addresses any elevated risks identified in a timely manner.

5. Periodic Reviews and Updates

5.1. Disqus conducts periodic reviews of its cloud computing use based on the cloud security alliance risks and controls structure and addresses any elevated risks identified in a timely manner.

5.2. Disqus promptly applies the latest firmware/security patches and updates on devices and software present in its network environment, expediting the application of critical and high-risk security patches and updates.

6. Encryption

6.1. Disqus ensures that all communications being initiated by Disqus or handling sensitive data are encrypted using industry-standard secure protocols.

B. Physical Security Measures

7. Data Center Security Measures

Disqus ensures appropriate data center physical security and data center environmental controls. Disqus utilizes the following physical security measures:

7.1. a closed-circuit television monitoring system with redundant power sources that provides recognizable images and usable recordings of entrances, exits, loading docks, and other high-security areas, and which maintains all images for at least 30 days and incident images indefinitely; The media portion is kept in a secured area.

7.2. distribution logs and for all issued access devices (including keys), secured storage areas for unissued devices, and regular audits of each of the foregoing;

7.3. access control alarms that actively are monitored by appropriate personnel;

7.4. identification (relying on governmentally issued credentials) and logging of individuals accessing Disqus' facilities (including visitors), as well as restriction of access to Publisher's assets (including intangible assets) to individuals authorized by Publisher.

C. Organizational Measures

8. Internal Employee Procedures and Policies

8.1. Role-based access control: Disqus maintains an up-to-date role-based access control based on data classification and job roles of employees, using the principle of least privilege and granting access only on a need-to-know basis.

8.2. Segregation of duties: Disqus maintains a segregation of duties, such that individuals performing application development are different from individuals managing production environments. Disqus employs technical and procedural controls to prevent developers and system administrators from obtaining access to production information.

8.3. Background checks: Disqus only utilizes personnel, including employees, contractors, and subcontractors, after performing background checks on them.

8.4. Security awareness training: Disqus ensures that its employees, contractors, and subcontractors receive appropriate security awareness training on a periodic basis.

8.5. Publisher's Standard of Conduct: If non-escorted access or access to Publisher systems is required, Disqus causes its representatives to comply with Publisher's standard of conduct.

9. Incident Response Plan

9.1. Disqus maintains an incident response plan that ensures that Disqus is adequately prepared to handle an incident, is able to accurately identify a Security Event as an incident, is able to contain the impact of the incident, has procedures in place to remediate the incident, has the ability to successfully recover from an incident and performs a root cause analysis of the incident.

10. Security Event

10.1. "Security Event" shall mean an instance of Disqus learning or having reason to believe that Publisher's confidential information has been accessed by an unauthorized person or disclosed in a manner not permitted by Disqus' agreement with Publisher, or that an incursion in any systems, processes, hardware or software used to store, transmit or that otherwise affect Publisher's confidential information has occurred.

10.2. In a Security Event, Disqus will:

10.2.1. as soon as reasonably practicable and in no event more than seventy-two hours after becoming aware of such Security Event, provide details of the same to Publisher including (i) the date of the Security Event, (ii) details concerning the data compromised, (iii) the method of the Security Event, (iv) appropriate Disqus security personnel contacts and security personnel contacts of its representatives, (v) the name of any person or entity assisting Disqus with the investigation of the suspected or actual Security Event, (vi) a list of all parties known to have gained unauthorized access to confidential information for the limited purpose of assessing Publisher's exposure and (vii) any other information which Publisher reasonably requests from Disqus or its representatives concerning such suspected or Security Event, including any forensics reports;

10.2.2. grant access to Publisher's representatives or another person or entity agreed to by Publisher and Disqus (with each acting in good faith in the selection of such other person or entity) to Disqus' systems and premises to allow such representatives or such other person or entity to perform an investigation (including the installation of any monitoring or diagnostic software) deemed necessary by Publisher to locate the source of such breach; and

10.2.3. immediately take appropriate steps to ensure that any actual data security breach does not continue.

10.3. Public Authorities: Disqus will not notify law enforcement or federal or state regulatory authorities of any Security Event or other matter related to Publisher's security requirements without prior notice to Publisher unless otherwise required by applicable law.

10.4. Press Releases: Disqus will not issue any press release or other public announcement concerning a Security Event without prior approval of Publisher.

10.5. Read-only logs: Disqus maintains usable read-only logs of critical systems and events on network devices, key security systems, and workstation and server operating systems, and ensures that any suspicious activity is monitored and investigated and appropriate actions are taken subsequent to its detection.

11. Data Classification

11.1. Classes: Disqus defines classes of data/information based on applicable legal requirements and sensitivity levels of the related data/information and treats such data/information according to that classification.

12. Collaboration with Publisher

12.1. Publisher's security requirements: If Publisher believes that Disqus' or any of its representatives' security procedures in connection with the services provided to Publisher do not comply with Publisher's security requirements, Disqus will cooperate with Publisher to ensure that security measures and procedures that comply with Publisher's security requirements are promptly implemented.

12.2. Notification: Disqus will promptly notify Publisher if Disqus learns or has reason to believe that it or any of its representatives are not in compliance with any of Publisher's security requirements, whether or not a Security Event has occurred.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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 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 – Optional: **Docking clause**

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8: **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

***Clause 10*: Data subject rights**

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

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

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

***Clause 11*: Redress**

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

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(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**

(c) [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 _____ (*specify Member State*).

***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 _____ (*specify Member State*).

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses: Use of the Disqus Commenting Platform.

Signature and date: _____

Role (controller): Controller

Data importer(s):

Name: Disqus, Inc.

Address: 3 Park Avenue, 33rd Floor, New York, NY 10016

Contact person's name, position and contact details: Steven Stein, steven.stein@disqus.com

Activities relevant to the data transferred under these Clauses: Providing the Disqus Commenting Platform.

Signature and date: _____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Users that use the Disqus comment function on a publisher's website

Categories of personal data transferred: SSO user data

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.

NA

The frequency of the transfer: Depends on user's use of the Disqus comment function.

Nature of the processing

Disqus provides a commenting application service ("Disqus Comments") to publisher for use as a comment forum on the publisher's website. Disqus collects personal data from users commenting in the Disqus Comments on publisher's website. Disqus provides publisher with access to the comments so that publisher may act as moderator on its website, and to meet its relevant obligations under applicable laws.

Purpose(s) of the data transfer and further processing: To fulfil user's request to comment on publisher's website.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As set forth in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

ANNEX II

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

A. Technical Measures

1. Information Security Policy

1.1 Disqus maintains a written information security policy which shall include, at a minimum, the approach adopted by Disqus to address the confidentiality, integrity, and availability of Disqus, its affiliates' and representatives', and its customers' confidential information, as applicable, which at least meets the minimum standards of (a) International Standard ISO.IEC 27001 and 27002 or (b) a similar industry-standard framework.

2. Testing and Scanning Procedures

2.1 Penetration testing: Upon request, Disqus provides Publisher with an executive summary of the results of penetration testing.

2.2 Information security certification: Upon request, Disqus provides Publisher with a third-party information security certification such as ISO 27K and SOC 2 Type II from an industry-recognized third party as of such then-completed year.

2.3 Vulnerability scanning: Upon request, Disqus provides Publisher with executive summaries of external, internal, and web application vulnerability scanning. If Publisher identifies elevated risks present within provided information, Disqus will promptly remediate identified risks at Disqus' expense. Disqus adheres to OWASP coding principles for web application code and uses static or dynamic application vulnerability scanning or manual code review, when appropriate. Disqus ensures that vulnerability scans periodically are conducted on devices and software present in its internal and external network environments and web applications to identify and remediate or have remediated any vulnerabilities within a documented timeframe. Disqus will provide Publisher with summaries of such scans and results upon request.

2.4 Penetration tests: Disqus conducts annual penetration tests on all its externally facing critical systems and applications from an industry-recognized independent third party at Disqus 'expense. Disqus conducts similar such tests after significant changes are made to its network. Such penetration tests shall:

(a) be based on industry-accepted penetration testing approaches (e.g. NIST SP800-115),
(b) include testing from inside and outside the network,
(c) include testing to validate segmentation, and
(d) include network-layer, operating system, and application layer testing such that, at a minimum, they test against vulnerabilities identified in industry standards (e.g. OWASP Guide, SANS CWE Top 25, CERT Secure Coding).

3. Backups

Disqus maintains secure, usable, and traceable data/information backups to ensure that backups can be used when necessary.

4. Internal Hardware Protection

4.1 Disqus ensures that all computing and storage devices on its network, including but not limited to, workstations, servers, and network devices have endpoint protection in place consistent with industry standards, such as anti-malware, email, and application scanning, or antivirus.

4.2 Disqus has a tiered network architecture, which includes preventive and detective devices and where highly sensitive non-public information is in a secured and segregated network.

4.3 Disqus ensures that the network devices, servers, and workstations where Publisher information is located are hardened and continuously subject to minimum security baselines.

4.4 Disqus maintains an inventory of authorized devices that can be connected to its network environment and ensures that such inventory is reconciled periodically.

4.5 Disqus maintains an inventory of authorized software required for its network devices, servers, and workstations present in its network environment and ensures that such inventory is reconciled periodically.

4.6 Disqus maintains a change management methodology that ensures only approved changes are released and deployed in the production environment.

4.7 Disqus conducts periodic reviews of its cloud computing use based on the cloud security alliance risks and controls structure and addresses any elevated risks identified in a timely manner.

5. Periodic Reviews and Updates

5.1 Disqus conducts periodic reviews of its cloud computing use based on the cloud security alliance risks and controls structure and addresses any elevated risks identified in a timely manner.

5.2 Disqus promptly applies the latest firmware/security patches and updates on devices and software present in its network environment, expediting the application of critical and high-risk security patches and updates.

6. Encryption

6.1 Disqus ensures that all communications being initiated by Disqus or handling sensitive data are encrypted using industry-standard secure protocols.

B. Physical Security Measures

7. Data Center Security Measures

Disqus ensures appropriate data center physical security and data center environmental controls. Disqus utilizes the following physical security measures:

7.1 a closed-circuit television monitoring system with redundant power sources that provides recognizable images and usable recordings of entrances, exits, loading docks, and other high-security areas, and which maintains all images for at least 30 days and incident images indefinitely; The media portion is kept in a secured area.

7.2 distribution logs and for all issued access devices (including keys), secured storage areas for unissued devices, and regular audits of each of the foregoing;

7.3 access control alarms that actively are monitored by appropriate personnel;

7.4 identification (relying on governmentally issued credentials) and logging of individuals accessing Disqus' facilities (including visitors), as well as restriction of access to Publisher's assets (including intangible assets) to individuals authorized by Publisher.

C. Organizational Measures

8. Internal Employee Procedures and Policies

8.1 Role-based access control: Disqus maintains an up-to-date role-based access control based on data classification and job roles of employees, using the principle of least privilege and granting access only on a need-to-know basis.

8.2 Segregation of duties: Disqus maintains a segregation of duties, such that individuals performing application development are different from individuals managing production environments. Disqus employs technical and procedural controls to prevent developers and system administrators from obtaining access to production information.

8.3 Background checks: Disqus only utilizes personnel, including employees, contractors, and subcontractors, after performing background checks on them.

8.4 Security awareness training: Disqus ensures that its employees, contractors, and subcontractors receive appropriate security awareness training on a periodic basis.

8.5 Publisher's Standard of Conduct: If non-escorted access or access to Publisher systems is required, Disqus causes its representatives to comply with Publisher's standard of conduct.

9. Incident Response Plan

9.1 Disqus maintains an incident response plan that ensures that Disqus is adequately prepared to handle an incident, is able to accurately identify a Security Event as an incident, is able to contain the impact of the incident, has procedures in place to remediate the incident, has the ability to successfully recover from an incident and performs a root cause analysis of the incident.

10. Security Event

10.1 "Security Event" shall mean an instance of Disqus learning or having reason to believe that Publisher's confidential information has been accessed by an unauthorized person or disclosed in a manner not permitted by Disqus' agreement with Publisher, or that an incursion in any systems, processes, hardware or software used to store, transmit or that otherwise affect Publisher's confidential information has occurred.

10.2 In a Security Event, Disqus will:

10.2.1 as soon as reasonably practicable and in no event more than seventy-two hours after becoming aware of such Security Event, provide details of the same to Publisher including (i) the date of the Security Event, (ii) details concerning the data compromised, (iii) the method of the Security Event, (iv) appropriate Disqus security personnel contacts and security personnel contacts of its representatives, (v) the name of any person or entity assisting Disqus with the investigation of the suspected or actual Security Event, (vi) a list of all parties known to have gained unauthorized access to confidential information for the limited purpose of assessing Publisher's exposure and (vii) any other information which Publisher reasonably requests from Disqus or its representatives concerning such suspected or Security Event, including any forensics reports;

10.2.2 grant access to Publisher's representatives or another person or entity agreed to by Publisher and Disqus (with each acting in good faith in the selection of such other person or entity) to Disqus' systems and premises to allow such representatives or such other person or entity to perform an investigation (including the installation of any monitoring or diagnostic software) deemed necessary by Publisher to locate the source of such breach; and

10.2.3 immediately take appropriate steps to ensure that any actual data security breach does not continue.

10.3 Public Authorities: Disqus will not notify law enforcement or federal or state regulatory authorities of any Security Event or other matter related to Publisher's security requirements without prior notice to Publisher unless otherwise required by applicable law.

10.4 Press Releases: Disqus will not issue any press release or other public announcement concerning a Security Event without prior approval of Publisher.

10.5 Read-only logs: Disqus maintains usable read-only logs of critical systems and events on network devices, key security systems, and workstation and server operating systems, and ensures that any suspicious activity is monitored and investigated and appropriate actions are taken subsequent to its detection.

11. Data Classification

11.1 Classes: Disqus defines classes of data/information based on applicable legal requirements and sensitivity levels of the related data/information and treats such data/information according to that classification.

12. Collaboration with Publisher

12.1 Publisher's security requirements: If Publisher believes that Disqus' or any of its representatives' security procedures in connection with the services provided to Publisher do not comply with Publisher's security

requirements, Disqus will cooperate with Publisher to ensure that security measures and procedures that comply with Publisher's security requirements are promptly implemented.

12.2 Notification: Disqus will promptly notify Publisher if Disqus learns or has reason to believe that it or any of its representatives are not in compliance with any of Publisher's security requirements, whether or not a Security Event has occurred.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

Exhibit C CPRA ADDENDUM

CPRA Addendum

Compliance with the California Consumer Privacy Act & Consumer Privacy Rights Act Regulations

Disqus Inc. ("**Disqus**") and the publisher identified in the main agreement (the "**Pulisher**") have one or more written agreements (collectively, "the **Agreement**") pursuant to which Disqus provides services to Publisher as a "Service Provider," a "Contractor," or a "Third Party" (as defined below). This addendum ("**CPRA Addendum**") shall apply to the extent that Disqus provides services to Publisher that fall under the scope of the CA Privacy Laws (as defined below).

It is the intent of the parties that Disqus acts as a Service Provider and/or a Contractor (as appropriate) for Publisher when it provides the services to Pulisher under the Agreement, provided that Disqus is a Service Provider or Contractor under the CA Privacy Laws. Disqus acts as a Third Party for Publisher when providing Cross-Contextual Behavioral Advertising or other services that CA Privacy Laws consider Third Party services.

This CPRA Addendum sets forth the requirements for contracts imposed upon the parties by the CA Privacy Laws (as defined below). This CPRA Addendum is hereby incorporated by reference into each Agreement to demonstrate the parties' compliance with the CA Privacy Laws.

1. Definitions.

   (a) "CA Privacy Laws" means, collectively, the California Consumer Privacy Act of 2018 ("**CCPA**", codified at Civil Code section 1798.100 *et seq*.), the California Privacy Rights Act ("**CPRA**"), and all applicable regulations issued by competent authorities that implement CCPA and CPRA. Words and phrases in this CPRA Addendum shall, to the greatest extent possible, have the meanings given to them in the CA Privacy Laws.

   (b) *"Contractor" has the meaning given to it in S*ection 1798.140(j) of the California Civil Code.

   (c) *"Service Provider" has the meaning given to it in S*ection 1798.140(ag) of the California Civil Code.

   (d) "Third Party" has the meaning given to it in Section 1798.140(ai) of the California Civil Code.

   (e) "Cross-Contextual Behavioral Advertising" has the meaning given to it in Section 1798.140(k) of the California Civil Code.

2. In accordance with § 7051 of the CPRA Regulations (Contract Requirements for Service Providers and Contractors), the following terms are incorporated by reference into the Agreement to the extent that Disqus acts as a Service Provider or Contractor:

   (a) Disqus is prohibited from selling or sharing personal information it collects pursuant to the Agreement. Disqus shall only process Publisher's personal information for the specific business purpose(s) set forth in the Agreement and for the specific business purposes listed below:

   - Providing advertising and marketing services and public relations of the Publisher's own business or activity, goods or services.
   - Providing a commenting platform to Publisher for Publisher's website.

(b) Disqus is prohibited from retaining, using, or disclosing the personal information that Disqus collected pursuant to the Agreement with the Publisher for any purposes other than those specified in this CPRA Addendum, the Agreement or as otherwise permitted by the CA Privacy Laws.

(c) Disqus is prohibited from retaining, using, or disclosing the personal information Disqus collected pursuant to the Agreement with the Publisher for any commercial purpose other than the business purposes specified in the Agreement, including in the servicing of a different business, unless expressly permitted by the CA Privacy Laws.

(d) Disqus is prohibited from retaining, using, or disclosing the personal information that Disqus collected pursuant to the Agreement with the Disqus outside the direct business relationship between Disqus and Publisher unless expressly permitted by the CA Privacy Laws. For example, Disqus may not combine or update personal information Disqus collected pursuant to the Agreement with the Publisher with personal information that it received from another source or collected from its own interaction with a consumer unless expressly permitted by the CA Privacy Laws.

(e) Disqus shall comply with all applicable sections of the CA Privacy Laws, including providing the same level of privacy protection as required by Publisher, by cooperating with Publisher in responding to and complying with consumers' requests made pursuant to the CA Privacy Laws, and implementing reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with California Civil Code section 1798.81.5.

(f) Disqus grants Publisher the right to take reasonable and appropriate steps to ensure that Disqus uses the personal information in a manner consistent with the Publisher's obligations under the CA Privacy Laws. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of Disqus's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.

(g) Disqus shall notify Publisher if Disqus can no longer meet its obligations under the CA Privacy Laws.

(h) Disqus grants Publisher the right, upon notice, to take reasonable and appropriate steps to stop and remediate Disqus's unauthorized use of personal information. Publisher may require Disqus to provide documentation that verifies that Disqus no longer retains or uses the personal information of consumers that have made a valid request to delete with the Publisher.

(i) Disqus shall enable Publisher to comply with consumer requests and Publisher shall notify Disqus of any consumer request made pursuant to the CA Privacy Laws that it must comply with and provide the information necessary for Disqus to comply with the request.

(j) To the extent that Disqus subcontracts with another person in providing services to Publisher, Disqus shall have a contract with the subcontractor that complies with the CA Privacy Laws.

3. In accordance with § 7053 of the CPRA Regulations (Contract Requirements for Third Parties), the following terms are incorporated by reference into the Agreement to the extent that Disqus acts as a Third Party:

(a) Disqus shall only process Publisher's personal information for the limited and specified business purpose(s) set forth in the Agreement and below.

- Cross-Context Behavioral Advertising: targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the Publisher's distinctly-branded website, application, or service with which the consumer intentionally interacts.

(b) Disqus shall comply with the CA Privacy Laws. Disqus shall provide the same level of privacy protection as required of Publisher. Disqus shall comply with a consumer's request to opt-out of sale/sharing forwarded to Disqus by a Publisher. Disqus shall implement reasonable security procedures and practices

appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(c) Disqus grants Publisher the right to take reasonable and appropriate steps to ensure that Disqus uses Publisher data in a manner consistent with the Publisher's obligations under the CA Privacy Laws. Publisher may require the Disqus to attest that Disqus treats Publisher data in the same manner that Publisher is obligated to treat it under the CA Privacy Laws.

(d) Disqus grants Publisher the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. Publisher may require Disqus to provide documentation that verifies that Disqus no longer retains or uses the personal information of consumers who have had their request to opt-out of sale/sharing forwarded to them by Publisher.

(e) Disqus shall notify Publisher if Disqus can no longer meet its obligations under the CA Privacy Laws.

4. Each party shall maintain records needed to demonstrate compliance with the applicable provisions of the CA Privacy Laws.

5. The CPRA Addendum shall remain in force so long as the Agreement is in force and shall terminate when the Agreement is terminated.