MaxMind Data Processing Addendum
(for MaxMind End User License Agreement)

This Data Processing Addendum ("Addendum") is referenced by and integrated into the MaxMind End User License Agreement ("Agreement") entered into by and between MaxMind, Inc. ("MaxMind) and various licensees (each referred to as a "Licensee" or "You"). MaxMind and you are sometimes referenced in this Addendum individually as a "party" and collectively, as the "parties".

This Addendum applies to the processing of Personal Information in connection with your use of the Services. Except to the extent otherwise expressly set forth in this Addendum, this Addendum is governed by the terms and conditions of the Agreement in which it is referenced. Any defined terms not otherwise defined herein shall have the meanings set forth in the Agreement. By agreeing to the Agreement, you acknowledge having read this Addendum and agree to be bound by its terms.

1. Definitions.

a. "Applicable Data Protection Law" means (i) the UK Data Protection Act 2018; (ii) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation" or "GDPR"); (iii) as of January 1, 2020, the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 *et seq*. ("California Consumer Privacy Act" or "CCPA"); and (iv) any other data protection laws, rules, regulations, self-regulatory guidelines, or implementing legislation applicable to a party's provision or use of the Services. For avoidance of doubt, any obligations relating to CCPA compliance shall not apply until January 1, 2020.

b. "controller," "business," "processor," "service provider," "data subject," "consumer," "processing," "sale," "sell," and "supervisory authority" (or any of the equivalent terms) each have the meaning set forth under Applicable Data Protection Law.

c. "EU Model Clauses" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of February 5, 2010 for the Transfer of Personal Information to Data Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision.

d. "Personal Information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, data subject, or household or is defined as "personally identifiable information," "personal information," "personal data," or similar term under Applicable Data Protection Law.

e. "Subprocessors" means subcontractors of MaxMind, which process Personal Information on behalf of MaxMind in connection with your use of the Services.

2. Processing of Personal Information.

a. Acknowledgement. You acknowledge and agree that MaxMind will process any and all Personal Information that you choose to make available to or through the Services or that you otherwise share with MaxMind in connection with your use of the Services.

b. MaxMind as a processor or service provider. In most circumstances, MaxMind processes Personal Information provided by you as a processor or service provider on your behalf. You are the controller or business which determines which Personal Information is relevant, and based on that analysis you instruct MaxMind on how to process Personal Information. Where MaxMind acts as a processor or service provider, MaxMind will comply with the obligations set out in Section 3 below.

c. MaxMind as a controller or business. In some circumstances, MaxMind processes Personal Information provided by you as an independent controller or business. For example, MaxMind processes and aggregates some of the Personal Information provided by you with data received from other sources (including other licensees) in order to improve the Services and provide you and other licensees with licensed data, more accurate information, robust risk score information, and the ability to flag potentially fraudulent activity, as applicable. Even after you stop using the Services, MaxMind will retain the Personal Information where it has a lawful basis, including for purposes of MaxMind's own legitimate interests of continuing to provide services for all licensees, complying with its legal obligations, resolving disputes, and enforcing its agreements. Where MaxMind acts as an independent controller or business, you shall also be an independent controller or business, and each party shall be individually responsible, as an independent controller or business, for its own processing of the Personal Information and compliance with Applicable Data Protection Law.

d. Website. To the extent you provide Personal Information through MaxMind's website (including in connection with correction requests), MaxMind will process the Personal Information in accordance with MaxMind's privacy policy available at https://www.maxmind.com/en/privacy-policy.

e. Your Receipt of Personal Information. In some instances, you may receive Personal Information from MaxMind that MaxMind maintains as an independent controller of business. For example, GeoIP Databases or GeoIP Data licensed to you may include Personal Information. Where you receive Personal Information from MaxMind, you agree that you will only process the Personal Information for the purposes set forth in the Agreement and in accordance with Applicable Data Protection Law. MaxMind and you are each an independent controller or business with respect to the Personal Information, and each party shall be

individually responsible for its own processing of the Personal Information and compliance with Applicable Data Protection Law. In the event that your receipt of the Personal Information constitutes a sale under Applicable Data Protection Law and you receive a "Do Not Sell" or opt-out of sale request from a consumer (whether directly from the consumer or relayed by MaxMind), you shall promptly cease any further use or sale of the applicable consumer's Personal Information upon its receipt of such request. You shall provide MaxMind with all assistance necessary for MaxMind to address any data subject or consumer rights or regulatory requests under Applicable Data Protection Law.

f. International Transfer. You acknowledge and agree that Personal Information will be stored and processed in the United States and other countries in which MaxMind or its service providers maintain facilities. By using the Services, you agree to the transfer of any Personal Information you provide to MaxMind outside of the country in which it was provided. For purposes of receiving Personal Information from the European Union, the United Kingdom, or Switzerland, MaxMind self-certifies to and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the U.S. Department of Commerce, and MaxMind shall maintain its self-certification to and compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to the processing of such transferred Personal Information. To the extent you receive Personal Information subject to the Privacy Shield Framework, in accordance with the Onward Transfer Principle, you agree to protect the Personal Information with at least the same level of protection as required by the Privacy Shield Principles. If you determine that you can no longer meet your obligations under this subsection, you shall promptly notify MaxMind of such determination and cease processing the Personal Information or take other reasonable and appropriate steps to remediate as required by MaxMind. As an alternative data transfer mechanism, the parties hereby enter into the EU Model Clauses attached hereto as Annex 1.

g. Your Obligations. MaxMind requires, and you hereby warrant and represent, that (i) you have provided any legally required notices and have a lawful basis for its sharing, transmission, and processing of Personal Information with, to, and by MaxMind; (ii) any Personal Information provided by you has not been collected, stored, or transferred to MaxMind in violation of any law, regulation, or contractual obligation applicable to you. You agree to maintain a privacy policy that complies with Applicable Data Protection Law and disclose your data practices relating to your use of the Services, provided that you shall not be required to expressly identify MaxMind unless otherwise required by Applicable Data Protection Law. You shall not make any representations or warranties to your users contrary to the terms and conditions in the Agreement. Without limiting the preceding sentence, if you make any representation or warranty to your users contrary to the terms and conditions in the Agreement, you shall be solely and exclusively responsible for such representation or warranty to the extent such representation or warranty differs from those in the Agreement and MaxMind shall have no liability for any such representation or warranty. As between MaxMind and you, you are responsible for all acts and omissions of your users in connection with their use of the Services, and you will reasonably cooperate with MaxMind in connection with any prohibited activities of

any user in connection with the Services. You will promptly notify MaxMind if you become aware of any such prohibited activities.

h. Liability. To the maximum extent permitted by applicable law, each party's liability is subject to the disclaimers, limitations of liability, and indemnification obligations in the Agreement.

3. Terms Applicable to MaxMind as a processor or service provider.

a. Application. When MaxMind processes Personal Information as a processor or service provider on your behalf (and not when MaxMind processes Personal Information as a controller or business), the terms in this Section 3 shall apply.

b. Instructions. You hereby instruct MaxMind to process Personal Information for the following purposes: (i) processing in accordance with the Agreement; (ii) processing initiated by your users in their use of the Services; and (iii) processing to comply with other documented reasonable instructions provided by you (*e.g.*, via email) where such instructions are consistent with the terms of the Agreement. MaxMind shall process the Personal Information only on documented instructions from you, unless required to do otherwise by applicable law to which MaxMind is subject; in such a case, MaxMind shall inform you of that legal requirement before processing the Personal Information, unless that law prohibits such disclosure on important grounds of public interest. The Agreement constitutes your complete and final documented instructions, and any additional or alternate instructions must be agreed upon separately.

c. Subject Matter, Duration, Data Subjects, and Types.

i. The subject matter of the processing is the performance of the Services to you pursuant to the Agreement.

ii. The duration of the processing is for the duration of the Agreement except where otherwise required by applicable law or legal obligation, or for MaxMind to protect its rights or those of a third party.

iii. The categories of data subjects or consumers about whom MaxMind processes Personal Information are determined and controlled by you, in your sole discretion, which may include, but are not limited to, your end users and your customers' end users.

iv. The types of Personal Information are determined and controlled by you, in your sole discretion, which may include, but are not limited to, IP address, email address, username and password, billing and shipping address, phone number, and transaction information.

d. CCPA. For any Personal Information subject to the CCPA, MaxMind shall not: (i) sell the Personal Information; (ii) retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services; (iii) retain, use, or disclose the Personal Information for a commercial purpose other than providing the Services; or (iv) retain, use, or disclose the information outside of the direct business relationship between MaxMind and you. MaxMind certifies that it understands these restrictions and will comply with them.

e. Subprocessors.

i. You hereby provide MaxMind with general written authorization to engage Subprocessors to assist in the performance of the Services. MaxMind shall enter into a written agreement with each Subprocessor containing data protection obligations no less protective than those in this Addendum with respect to the protection of Personal Information to the extent applicable to the services provided by the Subprocessor. MaxMind shall be liable for the acts and omissions of its Subprocessors to the same extent MaxMind would be liable if performing the services of each Subprocessor directly under the terms of the Agreement.

ii. MaxMind shall make available to you a current list of Subprocessors for the Services upon your written request. You may also make a written request that MaxMind notify you of any new Subprocessors. If you make such written request, MaxMind shall provide notification of new Subprocessors before authorizing any new Subprocessors to process Personal Information in connection with MaxMind's provision of the Services to you. You may object to MaxMind's use of a new Subprocessor by notifying MaxMind promptly in writing within ten (10) business days after receipt of MaxMind's notice. In the event you object to a new Subprocessor, MaxMind will use reasonable efforts to make available to you a change in the Services or recommend a commercially reasonable change to your configuration or use of the Services to avoid processing of the Personal Information by the objected-to new Subprocessors without unreasonably burdening you. If MaxMind is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, you may terminate the applicable Services which cannot be provided by MaxMind without the use of the objected-to new Subprocessor by providing written notice to MaxMind. MaxMind will refund you any prepaid fees covering the remainder of the term following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on you.

f. Requests. MaxMind shall, to the extent legally permitted, promptly notify you if MaxMind receives a request from a data subject or consumer to exercise their rights under Applicable Data Protection Law ("Request"). Taking into account the nature of the processing, MaxMind shall use commercially reasonable efforts to assist you in the fulfillment of your obligation to respond to the Request. To the extent legally permitted, you shall be responsible for any costs arising from MaxMind's provision of such assistance. You acknowledge and agree that MaxMind may not be able to fulfill a Request where to do so would violate laws applicable to MaxMind, would interfere with MaxMind's ability to meet legal obligations or protect its rights

or those of a third party, or would prevent MaxMind from continuing to process Personal Information where it has a legitimate interest in doing so.

g. Data Protection Impact Assessments. MaxMind shall provide you with reasonable cooperation and assistance as needed and appropriate to fulfill your obligations under Applicable Data Protection Law to carry out a data protection impact assessment related to your use of the Services, to the extent you do not otherwise have access to the relevant information, and to the extent such information is available to MaxMind. MaxMind shall provide reasonable assistance to you in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating the data protection impact assessment, to the extent required under Applicable Data Protection Law. To the extent legally permitted, you shall be responsible for any costs arising from MaxMind's provision of such assistance.

h. Audit. Subject to the confidentiality provisions set forth in the Agreement, you may make a written request at reasonable intervals that MaxMind make available to you a copy of MaxMind's then most recent third party audit with respect to its privacy and data protection practices, as applicable. If following MaxMind's delivery of such report you wish further information necessary to demonstrate MaxMind's compliance with its obligations as a processor or service provider, then MaxMind agrees at the written request from you to submit, to the extent reasonably possible, any facilities where it processes Personal Information on behalf of you for audit to ascertain compliance. Such audit shall be carried out upon the reasonable request of you, with reasonable notice, at reasonable intervals (no greater than once per year), during normal business hours, and subject to the confidentiality provisions set forth in the Agreement. You are responsible for and shall reimburse MaxMind for any expenses associated with the audit. You must receive written approval from MaxMind, at MaxMind's own discretion, before using any third party auditor, and such third party auditor must submit to a duty of confidentiality with respect to the audit.

i. Security. MaxMind shall maintain appropriate technical and organizational measures for the protection of the security, confidentiality, and integrity of Personal Information (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss, or alteration or damage, unauthorized disclosure of, or access to, Personal Information). MaxMind regularly monitors compliance with these measures. MaxMind will not materially decrease the overall security of the Services during its provision of the Services pursuant to the Agreement. MaxMind shall ensure that persons authorized to carry out processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality.

j. Incident Management and Notification. MaxMind maintains security incident management policies and procedures and shall notify you without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information transmitted, stored, or otherwise processed by MaxMind on behalf of you (a "Data Incident"). MaxMind shall make reasonable efforts to identify the cause

of such Data Incident and take steps as MaxMind deems necessary and reasonable in order to remediate the cause of such a Data Incident to the extent the remediation is within MaxMind's reasonable control. MaxMind shall have no responsibility to you for Data Incidents caused by you or your users.

k. Return and Deletion. Upon your written request, MaxMind will return or delete Personal Information processed by MaxMind on behalf of you. MaxMind may retain Personal Information where necessary for MaxMind to comply with applicable law or legal obligations, or to protect its rights or those of a third party.

Annex 1

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as ""Licensee" or "You" in the Agreement (the "data exporter**"**)

and

MaxMind, Inc., 14 Spring Street, Suite 3, Waltham, MA 02451, U.S.A.
(the "data importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the Agreement, the parties will be deemed to have signed this Appendix 1.

Data exporter
The data exporter is the entity identified as ""Licensee" or "You" " in the Agreement.

Data importer
The data importer is MaxMind, Inc.

Data subjects
Data subjects include the data exporter's end users and its customers' end users.

Categories of data
The personal data relating to individuals which is processed by the data importer through the data exporter's use of its services. The data exporter determines the types of data per each product or service used.

Processing operations
The personal data transferred will be subject to the following basic processing activities (as applicable):

- Providing fraud and risk analysis and Internet Protocol intelligence services and products.
- Providing technical support for and improvement to MaxMind services and products.
- Providing licensed data.
- Logging and backup.

The data importer may use subprocessors in connection with its processing activities for the data exporter.

MaxMind Data Processing Addendum
For MaxMind End User License Agreement
Version November 2019

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the Agreement, the parties will be deemed to have signed this Appendix 2.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c)

1. Risk Management.

- An annual Information Security risk assessment is performed covering MaxMind facilities and information assets.
- The risk assessment is conducted using an industry standard methodology (based on ISO 27002) to aid in identifying, measuring, and treating known risks.
- Risk assessment results and risk mitigation suggestions are shared with senior management.
- Our risk assessment results specify proposed changes to systems, processes, policies, or tools, in order to reduce security vulnerabilities and threats.

2. Security Policy.

- Policies, including those related to data privacy, security and acceptable use, are assessed and approved by MaxMind senior management. Policies are documented and published among all relevant personnel.
- Employees and contracted third parties are required to comply with MaxMind policies relevant to their scope of work.
- New employees receive training on confidentiality obligations, information security, compliance, and data protection.
- Employees receive regular training updates, which cover MaxMind Information Security policies and expectations.
- Where required, policies are supported by associated procedures, standards, and guidelines.
- Information Security policies are updated, as needed, to reflect changes to business objectives or risk.
- Senior management performs an annual review of all Information Security policies.

- Information Security policies are stored, maintained, updated, and published in a centralized, online location.

- MaxMind's Information Security Management System contains sections on password requirements, Internet usage, computer security, confidentiality, customer data protection, and Company data protection

3. Organization of Information Security.

- Information Security governance and data protection compliance for the Company are the responsibility of MaxMind's Vice President of Operations.

- MaxMind has established an Information Security team, with security responsibilities shared across various business units.

- Confidentiality and nondisclosure agreements are required when sharing sensitive, proprietary personal, or otherwise confidential information between MaxMind and a third-party.

- A formal process is in place to manage third parties with access to organizational data, information systems, or data centers. All such third parties commit contractually to maintaining confidentiality of all confidential information.

4. Asset Management.

- MaxMind assigns ownership for all information assets.

- MaxMind maintains an information assets classification policy and classifies such assets in terms of its value, legal requirements, sensitivity, and criticality to the organization.

- Desktops and laptops utilize encrypted storage partitions.

- MaxMind maintains a data disposal and destruction policy that covers the disposal of electronic assets and associated media.

5. Human Resources Information Security.

- Security roles and responsibilities for employees are defined and documented.

- MaxMind performs background screening of new hires including job history, references, and criminal checks (subject to local laws).

- MaxMind requires all new employees to sign employment agreements, which include comprehensive non-disclosure and confidentiality commitments.

- MaxMind maintains an information security awareness and training program that includes new hire training.

- Information Security awareness is enhanced through regular communications using company-wide emails, as necessary.

- The organization maintains attendance records for any formal security awareness training sessions.

- The Human Resources department notifies the Operations team about any changes in employment status and employment termination.

- MaxMind maintains a documented procedure for changes in employment status and employment termination (including notification, access modification, and asset collection). New third party service providers whose services involve access to any confidential information must agree contractually to data privacy and security commitments commensurate with their access and handling of confidential information.

- The MaxMind Privacy Policy include provisions related to the sharing of data with third party service providers and their obligations to maintain the confidentiality of that data.

6. Physical and Environmental Security.

- Physical security controls in all data centers utilized by MaxMind, in providing the Service, include protection of facility perimeters using various access control measures (including biometric identification, supervised entry, 24/7/365 on-premise security teams, CCTV systems).

- Access to data centers is limited to authorized employees or contractors only.

- Controls are in place to protect against environmental hazards at all data centers.

- All data center facilities have successfully been attested to SSAE 16, SOC 2 type 2, ISO 27001, or similar requirements.

7. Communications and Operations Management.

- The operation of systems and applications that support the Service is subject to documented operating procedures.

- The System Administration team maintains standard server configurations.
- Separate environments are maintained to allow for the testing of changes.
- Third-party access to MaxMind systems is regularly audited.
- The organization maintains documented backup procedures. Full backups are performed regularly for all production databases. Data backups are transferred to an offsite location on a regular schedule and are stored encrypted.
- All systems and network devices are synchronized to a reliable and accurate time source via the "Network Time Protocol" (NTP).
- All high priority event-alerting tools escalate into notifications for MaxMind's 24x7 incident response teams, providing the System Administration team with alerts, as needed.

8. Access Controls.

- MaxMind maintains an "Acceptable Use" policy that outlines requirements for the use of user IDs and passwords.
- The organization publishes and maintains a password management standard. In general, users are asked to follow the strong password policies.
- Strong authentication practices (e.g., SSH keys, 2FA, IP based restrictions) are used to control access to production and development environments.
- Direct access to the "root" account on all production servers is restricted to Software Engineering and System Administration personnel deemed necessary.
- All access controls are based on "least privilege" and "need to know" principles. Different roles, including limited and administrative access, are used in the environment.
- Upon notice of termination, all user access is removed. All critical system access is removed immediately upon notification.

9. Information Systems Acquisition, Development, and Maintenance.

- Product features are managed through a formalized product management process. Security requirements are discussed and formulated during scoping and design discussions.

- MaxMind maintains a QA Department dedicated to reviewing and testing application functionality and stability.

- Application source code is stored in a central repository. Access to source code is limited to authorized individuals.

- Changes to MaxMind software are tested before production deployment. Deployment processes include unit testing at the source environment, as well as integration and functional testing within a test environment prior to implementation in production.

10. Information Security Incident Management.

- MaxMind maintains an incident response process.

- Internally, MaxMind maintains an incident response plan that is tested on a regular basis. The plan addresses specific incident response procedures, data backup procedures, roles and responsibilities, customer communication, contact strategies, and legal information flow.

- The incident response plan is exercised on a regular basis, at least annually.

11. Business Continuity Management.

- For redundancy, MaxMind utilizes database replication architectures.

- Database backups are stored on local disks in data centers, as well as copied to remote storage locations.

- MaxMind has implemented redundant data center infrastructure to better support high availability across the entire system. Each key service layer includes redundant components that mitigate the impact of predictable failures such as hardware problems, and also allows for capacity scaling as customer data and usage grows.

12. MaxMind Application Security Features.

- Access to MaxMind services requires access to a unique license key, and access to a customer's account portal requires a login and password. MaxMind supports and encourages use of HTTPS for all communications with our website and services.