MaxMind Data Processing Addendum

(Revised November 2021)

This Data Processing Addendum (“Addendum”) is referenced by and integrated into the MaxMind End User License Agreement, License Agreement, Reseller Agreement, OEM Agreement or GeoLite2 End User License Agreement (each an “Agreement”) entered into by and between MaxMind, Inc. (“MaxMind) and the customer defined therein as “you,” “Licensee,” or “Reseller” (“you”) and execution of the Agreement is understood by the parties and shall be deemed as execution of this Addendum and the Standard Contractual Clauses, as applicable. 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. For purposes of this Addendum, the term “end users” includes, without limitation, your customers and their end users, as applicable. By agreeing to the Agreement, you acknowledge having read this Addendum and agree to be bound by its terms. MaxMind may revise this Addendum as necessary to address changes to Applicable Data Protection Law or MaxMind policies, and such changes shall be binding and effective upon the earlier of (i) the date that is thirty (30) days after the posting of the revised Addendum or (ii) the date that MaxMind provides notice to you of the revised Addendum.

1. Definitions.

a. “Applicable Data Protection Law” means (i) European Data Protection Law (ii) the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 et seq. (“CCPA”); (iii) The Brazilian Data Protection Law, Law N. 13.709 from August 14th, 2018 (“LGPD”); (iv) the People’s Republic of China (“PRC”) Personal Information Protection Law (“PIPL”) and (v) any other data protection laws, rules, regulations, self-regulatory guidelines, or implementing legislation applicable to a party’s provision or use of the Services.

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. “Personal Information” means information that identifies, relates to, describes, is reasonably 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.

d. "European Data Protection Law" means (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing
Directive 95/46/EC (General Data Protection Regulation) ("GDPR"); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Data Protection Act ("Swiss DPA"), in each case as may be supplemented, updated or superseded from time to time.

e. " Restricted Transfer" means: (i) where the GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner, and (iv) where LGPD applies, a transfer of personal data from Brazil to a country outside of Brazil which does not provide an adequate level of protection within the meaning of LGPD.

f. "Standard Contractual Clauses" means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs").

g. “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 You Provide

a. Acknowledgement. You acknowledge and agree that MaxMind will process Personal Information that you provide to MaxMind in connection with your use of the Services, including in the United States and other countries in which MaxMind or its service providers maintain facilities. For the current list of facilities MaxMind and its service providers maintain, please submit a written request to support@maxmind.com. For the avoidance of doubt, MaxMind does not undertake any processing of Personal Information provided by you in connection with its provision of the GeoIP Databases or GeoLite2 Databases and, therefore, the Section 6 of this Addendum shall not apply to MaxMind's provision of GeoIP Databases or GeoLite2 Databases to You.

b. MaxMind as a Processor or Service Provider. Subject to Section 2(c), MaxMind processes Personal Information provided by you in connection with your use of the Services 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 on your behalf, the parties will comply with the obligations set out in Section 6 below.
c. **MaxMind as a Controller or Business.** In some circumstances, MaxMind processes Personal Information provided by you as an independent controller or business and you hereby authorize such use of Personal Information. 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 for its own processing of the Personal Information and compliance with Applicable Data Protection Law. In the event that MaxMind’s receipt of Personal Information from you is deemed a sale under the CCPA, you will ensure that you comply with your obligations as a business under the CCPA.

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](https://www.maxmind.com/en/privacy-policy).

3. **Processing of Personal Information You Receive.** You acknowledge and agree that you may receive Personal Information from MaxMind in connection with your use of the Services, and that such information may relate to data subjects or consumers across jurisdictions (including from the European Economic Area, Switzerland, the United Kingdom and Brazil). 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 is deemed a sale under the CCPA and you receive a “Do Not Sell” 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 your 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.

4. **Your Obligations.** MaxMind requires, and you hereby represent and warrant, that (i) you have provided any legally required notices and choice, and have a lawful basis for your sharing, transmission, and processing of Personal Information from, with, to, and by MaxMind; (ii) you have complied with all data transfer requirements of any applicable jurisdictions, and any data transfers pursuant to this Addendum will not cause MaxMind to be in breach of Applicable Data Protection Law; and (iii) 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 end users contrary to the terms and conditions in the Agreement. Without limiting the preceding sentence, if you make any representation or warranty to your end 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 end users in connection with their processing of Personal Information, and you will reasonably cooperate with MaxMind in connection with any prohibited activities of any end user in connection with the Services. You will promptly notify MaxMind if you become aware of any such prohibited activities. In the event that the Standard Contractual Clauses are invalidated by a competent governmental authority, you will work with MaxMind to find an alternative legal basis for the transfer and continued processing of Personal Information in compliance with Applicable Data Protection Law, and you will cease processing Personal Information in the event no such basis is found or agreed upon by MaxMind.

5. **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.

6. **Terms Applicable to MaxMind as a Processor or Service Provider.**

   a. **Application.** When MaxMind processes Personal Information you provide 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 6 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 end 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. Where MaxMind follows your instructions, you will ensure that your instructions will not cause MaxMind to violate any applicable laws, rules, or regulations, or contractual obligations.

   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.

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, as set out in Schedule 2 hereto with changes being permitted pursuant to Section 6(e)(ii) below. 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 provide notification of new Subprocessors no less than fifteen (15) business days before authorizing any new Subprocessors to process Personal Information in connection with MaxMind’s provision of the Services to you. In order to receive such notifications, you must sign up by written request to MaxMind. 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), including as further set out in Schedule 3 hereto. MaxMind regularly monitors compliance with these measures and may update such measures from time to time, so long as such updates will not materially decrease the overall security of the Services during the 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 end 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.

7. **International Transfers of Personal Information**

a. The parties agree that in the event any transfer of Personal Information from you (as "data exporter") to MaxMind (as "data importer") is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this Addendum, as follows:

   i. In relation to transfers of Personal Information that is protected by the EU GDPR and processed in accordance with Section 2(b) of this Addendum, the EU SCCs shall apply, completed as follows:

   A. Module Two or Module Three will apply (as applicable);
   B. in Clause 7, the optional docking clause will apply;
   C. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 6(e)(ii) of this Addendum;
   D. in Clause 11, the optional language will not apply;
   E. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
   F. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
   G. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1.1 to this Addendum; and
   H. Subject to section 6(i) of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 3 to this Addendum;

   ii. In relation to transfers of personal data protected by the EU GDPR and processed in accordance with Section 2(c) of this DPA, the EU SCCs shall apply, completed as follows:

   A. Module One will apply;
   B. in Clause 7, the optional docking clause will apply;
   C. in Clause 11, the optional language will not apply;
D. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

E. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

F. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1.2 to this Addendum; and

G. Subject to the language provided in Section 6(i) of this Addendum, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 3 to this Addendum;

iii. In relation to transfers of personal data protected by the UK GDPR or the Swiss DPA or LGPD, the EU SCCs will also apply in accordance with paragraphs (i) and (ii) above, with the following modifications:

A. references to "Regulation (EU) 2016/679" shall be interpreted as references to UK GDPR or the Swiss DPA or LGPD (as applicable);

B. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the UK GDPR or the Swiss DPA or LGPD (as applicable);

C. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to the "UK" or "Switzerland" or “Brazil”, or "UK law" or "Swiss law" or “Brazilian law” (as applicable);

D. the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland or Brazil from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland or Brazil);

E. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner or Brazil Data Protection Authority (as applicable);

F. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" or the “Brazil Data Protection Authority” and “courts of Brazil” (as applicable);

G. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland or Brazil (as applicable); and

H. with respect to transfers to which UK GDPR applies, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved
by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland,

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such personal data in compliance with the UK GDPR or Swiss DPA in which case the UK SCCs or the Swiss SCCs (as applicable) shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs or the Swiss SCCs shall be populated using the information contained in Schedules 1.1, 1.2 and 3 of the Addendum (as applicable);

b. The parties agree that in the event any transfer of Personal Information from MaxMind (as "data exporter") to you (as "data importer") is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this Addendum, as follows:

   i. In relation to transfers of personal data protected by the EU GDPR and processed in accordance with Section 3 of this Addendum, the EU SCCs shall apply, completed as follows:
      
      A. Module One will apply;
      
      B. in Clause 7, the optional docking clause will apply;
      
      C. in Clause 11, the optional language will not apply;
      
      D. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
      
      E. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
      
      F. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 4 to this Addendum; and
      
      G. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 5 to this Addendum;

   ii. In relation to transfers of personal data protected by the UK GDPR or the Swiss DPA or LGPD, the EU SCCs will also apply in accordance with paragraph (i) above, subject to the same modifications as are described in Section 7(a)(iii); unless the EU SCCs, implemented as described in this Section 7(b)(ii), cannot be used to lawfully transfer such Personal Information in compliance with the UK GDPR or Swiss DPA in which case the UK SCCs or the Swiss SCCs (as applicable) shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes or
Appendices of the UK SCCs or the Swiss SCCs shall be populated using the information contained in Schedules 4 and 5 of the Addendum (as applicable);

c. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this Addendum) the Standard Contractual Clauses shall prevail to the extent of such conflict.

d. The parties agree that in the event that any transfer of Personal Information from you to MaxMind is subject to PIPL or other PRC laws and standards, that you shall secure separate consent and/or comply with the other requirements under PIPL and other PRC laws and standards that may apply. To the extent that any transfer of Personal Information from you to MaxMind is subject to PIPL, the purpose, period and processing method are as set forth in Schedules 1.1 and 1.2 and the security protection measures to be taken by MaxMind are set forth in Schedule 3.

8. Execution and Entry into Force. The parties agree that this Addendum (and the Standard Contractual Clauses, as applicable) are referenced in and form an integral part of the Agreement and execution of the Agreement shall be deemed to include execution of this Addendum and the Standard Contractual Clauses (as applicable), to the extent required by applicable law.
### Schedule 1.1

**Description of Processing / Transfer**

**Modules 2 and 3 (controller/processor to processor transfers)**

#### A. LIST OF PARTIES

**Data exporter(s):**

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Party identified as “you” in the Addendum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Address</td>
<td>The notice address provided by you to MaxMind</td>
</tr>
<tr>
<td></td>
<td>Contact person’s name, position and contact details:</td>
<td>The contact person, their position and contact details provided by you to MaxMind.</td>
</tr>
<tr>
<td></td>
<td>Activities relevant to the data transferred under these Clauses:</td>
<td>Providing data for the purpose of utilizing the Services.</td>
</tr>
<tr>
<td></td>
<td>Role:</td>
<td>Controller/ Processor</td>
</tr>
</tbody>
</table>

**Data importer:**

<table>
<thead>
<tr>
<th></th>
<th>Name:</th>
<th>MaxMind, Inc.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Address:</td>
<td>14 Spring Street #3, Waltham MA 02451, USA</td>
</tr>
<tr>
<td></td>
<td>Contact person’s name, position and contact details:</td>
<td>MaxMind, Inc. Legal Department email: <a href="mailto:legal@maxmind.com">legal@maxmind.com</a></td>
</tr>
</tbody>
</table>
|   | Activities relevant to the data transferred under these Clauses: | Providing the Services described in the Agreement. For example:  
  - For minFraud: Providing fraud and risk analysis and data relating to IP Addresses intelligence.  
  - For GeoIP2 Precision Service and GeoLite Web Service: Providing data relating to IP Addresses.  
  - For GeoIP2 Precision Service, minFraud Service and GeoLite2 Web Service: Providing technical support for and improvement to the Services, logging and backup |
|   | Role: | Processor |
### B. DESCRIPTION OF TRANSFER

| Categories of data subjects whose personal data is transferred: | End users of the data exporter and those of its customers, business partners, and other third parties. |
| Categories of personal data transferred: | The personal data transferred is based on the products or services used pursuant to the Agreement, which may include, but is not limited to the following categories of personal data:  
- For GeoIP2 Precision Service and GeoLite2 Web Service: IP Addresses  
- For minFraud Service: IP Addresses, network, postal code level or less precise level geolocation data, name and email address. |
| 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: | No sensitive data will be transferred. |
| The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): | Continuous - the data will be transferred periodically over the term of the Agreement. |
| Nature of the processing: | 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. |
<p>| Purpose(s) of the data transfer and further processing: | For purposes based on the Services used pursuant to the Agreement, including providing IP Geolocation services, fraud detection and related services. |</p>
<table>
<thead>
<tr>
<th><strong>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:</strong></th>
<th>Personal data is deleted within 30 days for data submitted to the GeoIP Precision Service, within 4 months for data submitted to the minFraud Service determined by MaxMind to have a low-risk score, and within 15 months for data submitted to the minFraud Service determined by MaxMind to have a high-risk score.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:</strong></td>
<td>Google, Inc. hosts MaxMind’s data center infrastructure for so long as MaxMind retains the data. Cloudflare, Inc. provides DNS and security for the Services and the duration of Cloudflare’s processing for each query or interaction with MaxMind’s website lasts less than one second.</td>
</tr>
</tbody>
</table>

## C. COMPETENT SUPERVISORY AUTHORITY

| Identify the competent supervisory authority/ies in accordance with Clause 13 of the EU SCCs (where applicable) | For transfers to which the GDPR applies – the competent supervisory authority will be determined in accordance with the criteria set forth in Clause 13 of the EU SCCs, provided that if the data exporter is not established in an EU Member State and has not appointed a representative, the Irish Supervisory Authority shall act as the competent supervisory authority. For transfers to which LGPD applies the competent supervisory authority is the Brazil Data Protection Authority. For transfers to which the UK GDPR applies the competent supervisory authority is the UK Information Commissioner's Office. For transfers to which the Swiss DPA applies the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner. |
### Schedule 1.2

**Description of Processing / Transfer**

**Module 1 (controller to controller transfers)**

#### A. LIST OF PARTIES

**Data exporter(s):**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Name:</td>
<td>Party identified as “You” in the Addendum</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>The notice address provided by you to MaxMind.</td>
<td></td>
</tr>
<tr>
<td>Contact person’s name, position and contact details:</td>
<td>The contact person, position and contact details provided by you to MaxMind.</td>
<td></td>
</tr>
<tr>
<td>Activities relevant to the data transferred under these Clauses:</td>
<td>Providing data for the purpose of utilizing the Services and allowing service improvement.</td>
<td></td>
</tr>
<tr>
<td>Role:</td>
<td>Controller</td>
<td></td>
</tr>
</tbody>
</table>

**Data importer:**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Name:</td>
<td>MaxMind, Inc,</td>
<td></td>
</tr>
<tr>
<td>Address:</td>
<td>14 Spring Street #3 Waltham MA 02451, USA</td>
<td></td>
</tr>
<tr>
<td>Contact person’s name, position and contact details:</td>
<td>MaxMind, Inc. Legal Department email: <a href="mailto:legal@maxmind.com">legal@maxmind.com</a></td>
<td></td>
</tr>
<tr>
<td>Activities relevant to the data transferred under these Clauses:</td>
<td>Improvement of Services</td>
<td></td>
</tr>
<tr>
<td>Role:</td>
<td>Controller</td>
<td></td>
</tr>
</tbody>
</table>

#### B. DESCRIPTION OF TRANSFER

<table>
<thead>
<tr>
<th>Categories of data subjects whose personal data is transferred:</th>
<th>End users of the data exporter and those of its customers, business partners, and other third parties.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of personal data transferred:</td>
<td>The personal data transferred is based on the products or services used pursuant to the Agreement, which may include, but is not limited to the following categories of personal data:</td>
</tr>
<tr>
<td></td>
<td>• For GeoIP2 Precision Service and GeoLite2 Web Service: IP Addresses</td>
</tr>
</tbody>
</table>
- For minFraud Service: Categories of personal data transferred may include, but are not limited to IP address, network, postal code level or less precise level geolocation data, name and email address.

<table>
<thead>
<tr>
<th>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:</th>
<th>No sensitive data will be transferred.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):</td>
<td>Continuous - the data will be transferred periodically over the term of the Agreement.</td>
</tr>
<tr>
<td>Nature of the processing:</td>
<td>MaxMind processes and aggregates personal data provided by you with data received from other sources (including other licensees) for the purpose of improving the Services and providing you and other licensees with licensed data, more accurate information, robust risk score information, and the ability to flag potentially fraudulent activity.</td>
</tr>
<tr>
<td>Purpose(s) of the data transfer and further processing:</td>
<td>For the purpose of improving the Services.</td>
</tr>
<tr>
<td>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:</td>
<td>Personal data is deleted within 30 days for data submitted to the GeoIP Precision Service, within 4 months for data submitted to the minFraud Service determined by MaxMind to have a low-risk score, and within 15 months for data submitted to the minFraud Service determined by MaxMind to have a high-risk score.</td>
</tr>
<tr>
<td>For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:</td>
<td>Google, Inc. hosts MaxMind’s data center infrastructure for so long as MaxMind retains the data. Cloudflare, Inc. provides DNS and security for the Services and the duration of Cloudflare’s processing for each query or interaction with MaxMind’s website lasts less than one second.</td>
</tr>
</tbody>
</table>

### C. COMPETENT SUPERVISORY AUTHORITY

| Identify the competent supervisory authority | For transfers to which the GDPR applies – the |
authority/ies in accordance with Clause 13 of the EU SCCs (where applicable)

<table>
<thead>
<tr>
<th></th>
<th>competent supervisory authority will be determined in accordance with the criteria set forth in Clause 13 of the EU SCCs, provided that if the data exporter is not established in an EU Member State and has not appointed a representative, the Irish Supervisory Authority shall act as the competent supervisory authority. For transfers to which LGPD applies the competent supervisory authority is the Brazil Data Protection Authority. For transfers to which the UK GDPR applies the competent supervisory authority is the UK Information Commissioner's Office. For transfers to which the Swiss DPA applies the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.</th>
</tr>
</thead>
</table>
## Schedule 2
### Subprocessors

<table>
<thead>
<tr>
<th>Subprocessor</th>
<th>Brief Description of Processing</th>
<th>Datacenter Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google, Inc.</td>
<td>Google Cloud Storage - Cloudstorage provider</td>
<td>Iowa, USA</td>
</tr>
<tr>
<td>Google, Inc.</td>
<td>Google Cloud Platform - Cloud infrastructure provider</td>
<td>Iowa, USA Oregon, USA N. Virginia, USA UK Singapore</td>
</tr>
</tbody>
</table>
Schedule 3

Minimum Technical and Organization Measures

1. Risk Management.
   ● A continuous 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 27001) to aid in identifying, measuring, and treating known risks.
   ● Risk assessment results and risk mitigation suggestions are shared with senior management.
   ● Risk assessment results specify proposed changes to systems, processes, policies, or tools, in order to reduce security vulnerabilities and threats.
   ● A Data Protection Officer (DPO) who is independent, regularly reviews data protection risks and controls.

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 MaxMind data protection.
3. **Organization of Information Security.**

- Information Security governance and data protection compliance for MaxMind are the responsibility of MaxMind’s Chief Operating Officer.
- 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 full disk encryption.
- 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 includes provisions related to the sharing of data with third party service providers and their obligations to maintain the confidentiality of that data.

- Physical security controls in all data centers utilized by MaxMind, in providing the Service, include multiple physical security layers including biometric identification, metal detectors, supervised entry, 24/7/365 on-premise security teams, CCTV systems, vehicle barriers, and laser based intrusion detection 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 Site Reliability Engineer (SRE) 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 SRE team with alerts, as needed.
- Network security controls that provide for the use of native cloud firewall technology, Virtual Private Cloud (VPC) architecture with strict trust boundaries, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

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. Password controls are designed to manage and control password strength, and usage including prohibiting users from sharing passwords.

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 “deny by default”, “least privilege” and “need to know” principles. Different roles, including limited and administrative access, are used in the environment.

System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

Upon notice of termination, all user access is removed. All critical system access is removed immediately upon notification.


- 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.
- Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to MaxMind technology and information assets.
- Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
- Formal Vendor Management program, including vendor security reviews for critical vendors to ensure compliance with MaxMind Information Security Policies.

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.

- Incident management procedures are designed to allow MaxMind to investigate, respond to, mitigate and notify of events related to MaxMind technology and information assets.
- The incident response plan is exercised on a regular basis, at least annually.

- Business resiliency/continuity procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.
- 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.

- 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.
- Communication with MaxMind’s services utilizes cryptographic protocols such as TLS to protect information in transit over public networks. At the network edge, bot management, web application firewalls, and DDoS protection are used to filter attacks. Within the internal network, applications follow a multi-tiered model which provides the ability to apply security controls between each layer.
- Data security controls which include logical segregation of data, restricted (e.g. role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.
- Personal data submitted via the minFraud Service is tokenized so the data can no longer be attributed to a specific individual without the use of additional information. The tokenized data and the additional information are stored separately and subject to access controls described above.

13. Data Privacy and Protection Measures
- MaxMind has implemented policies and processes to ensure that personal data is processed appropriately throughout its lifecycle (from collection through to use, retention, disclosure and destruction).
- MaxMind has implemented a data subject requests process to uphold data subject rights in
accordance with applicable data protection laws. MaxMind is committed to upholding these rights and ensuring that MaxMind responds to data subject requests in a transparent, fair, ethical and lawful way.

- MaxMind maintains a record of all data subject requests received and the actions taken to respond to these requests. MaxMind will provide all reasonable support to customers in responding to data subject requests, where requested, and in accordance with the agreements with them.

- MaxMind’s processors are required to sign appropriate agreements that govern the processing and protection of personal data and require the same obligations, as outlined in the Addendum, to be transferred to any further processors who MaxMind may engage. MaxMind has undertaken all reasonable efforts to ensure that Data Processing Agreements are in place with its processors.

- MaxMind relies on Standard Contractual Clauses to support the lawful transfer of personal data outside of the country where it was originally collected and have appropriate agreements in place with MaxMind subsidiaries, affiliates, processors, sub-processors and clients to support cross-border transfers.
### Schedule 4

**Description of Processing / Transfer**

**Module 1 (controller to controller transfers)**

A. **LIST OF PARTIES**

<table>
<thead>
<tr>
<th>Data exporter(s):</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Name:</strong></td>
<td>MaxMind, Inc.</td>
</tr>
<tr>
<td><strong>Address:</strong></td>
<td>14 Spring Street #3 Waltham MA 02451, USA</td>
</tr>
<tr>
<td><strong>Contact person’s name, position and contact details:</strong></td>
<td>MaxMind, Inc. Legal Department email: <a href="mailto:legal@maxmind.com">legal@maxmind.com</a> MaxMind DPO email: <a href="mailto:dpo@maxmind.com">dpo@maxmind.com</a> MaxMind, Inc. Data Protection Officer 14 Spring Street, 3rd Floor Waltham MA 02451, USA GDPR Representative Online request form: <a href="https://edpo.com/gdpr-data-request/">https://edpo.com/gdpr-data-request/</a> EDPO Block 1, Blanchardstown Corporate Park, Ballycoolin Rd, Dublin D15 AKK1, Ireland UK GDPR Representative Online request form: <a href="https://edpo.com/uk-gdpr-data-request/">https://edpo.com/uk-gdpr-data-request/</a> EDPO UK 8 Northumberland Avenue, London WC2N 5BY, United Kingdom</td>
</tr>
</tbody>
</table>

| Activities relevant to the data transferred under these Clauses: | Providing the Services described in the Agreement. |
| Role: | Controller |

#### Data importer(s):

<table>
<thead>
<tr>
<th>1. Name:</th>
<th>Party identified as “you” in the Addendum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>The notice address provided by you to MaxMind</td>
</tr>
<tr>
<td><strong>Contact person’s name, position and contact details:</strong></td>
<td>The contact person, position and contact details provided by you to MaxMind.</td>
</tr>
</tbody>
</table>
### Activities relevant to the data transferred under these Clauses:

| Role: | Controller |

### B. DESCRIPTION OF TRANSFER

<table>
<thead>
<tr>
<th>Categories of data subjects whose personal data is transferred:</th>
<th>Individuals associated with IP Addresses supplied by MaxMind</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of personal data transferred:</td>
<td>IP Addresses and associated data</td>
</tr>
<tr>
<td>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:</td>
<td>No sensitive data will be transferred.</td>
</tr>
<tr>
<td>The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):</td>
<td>Continuous - the data will be transferred periodically over the term of the Agreement.</td>
</tr>
<tr>
<td>Nature of the processing:</td>
<td>Transmission of data to You for Your purposes as permitted in the Agreement.</td>
</tr>
<tr>
<td>Purpose(s) of the data transfer and further processing:</td>
<td>For purposes based on the Services used pursuant to the Agreement, including providing IP Geolocation services, fraud detection and related services.</td>
</tr>
<tr>
<td>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:</td>
<td>Data may be retained for the periods specified in the Agreement.</td>
</tr>
<tr>
<td>For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### C. COMPETENT SUPERVISORY AUTHORITY

| Identify the competent supervisory authority/ies in accordance with Clause 13 of the EU SCCs (where applicable) | Irish Supervisory Authority |
## Schedule 5

### Technical and Organizational Security Measures

<table>
<thead>
<tr>
<th>Measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measures of pseudonymisation and encryption of personal data</td>
<td>You will ensure that you support the following encryption measures when utilizing MaxMind’s Services:</td>
</tr>
<tr>
<td></td>
<td>• HTTPS encryption for data in transit using TLS 1.2 AES-256-GCM or TLS 1.3 AES-128-GCM on every login interface and every information system network communication channel.</td>
</tr>
<tr>
<td></td>
<td>• Full Disk Encryption of data at rest using the industry standard AES-256-GCM algorithm.</td>
</tr>
<tr>
<td>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</td>
<td>• Ensure that all account users have strong, secure passwords that are updated regularly.</td>
</tr>
<tr>
<td></td>
<td>• Review users and permissions regularly if you make use of multi-user account access.</td>
</tr>
<tr>
<td></td>
<td>o Do not share user accounts and passwords, and deactivate any user accounts if no longer used.</td>
</tr>
<tr>
<td></td>
<td>• Treat your license key like a password, and store it securely (e.g. in a password manager)</td>
</tr>
<tr>
<td></td>
<td>• Logging in place for all information systems to record sufficient information to serve the operational needs, preserve accountability, and detect malicious activity.</td>
</tr>
<tr>
<td></td>
<td>• Resilience measures including redundancy built into your infrastructure and service architecture, as well as adequate protecting your backups.</td>
</tr>
<tr>
<td></td>
<td>• For automating GeoIP downloads, use GeoIP Update version 3.1.1 or greater.</td>
</tr>
<tr>
<td>Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident</td>
<td>• Continuity Planning and Disaster Recovery Plan</td>
</tr>
<tr>
<td></td>
<td>• Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents.</td>
</tr>
<tr>
<td>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in</td>
<td>• Regular testing of emergency equipment, technical controls, and processes.</td>
</tr>
</tbody>
</table>
| Measures for user identification and authorisation | • Secure network interconnections ensured by VPN, MFA, firewalls etc.  
• Logging of transmissions of data from information systems that stores or processes personal data.  
• Logging authentication and monitored system access.  
• Access to data necessary for the performance of the particular task is ensured within the information systems and applications by a corresponding role and authorization concept in accordance to the “need-to-know” principle. |
| Measures for the protection of data during transmission | • HTTPS encryption for data in transit using TLS v1.2+ or greater.  
• For automating GeoIP downloads, use GeoIP Update version 3.1.1 or greater. |
| Measures for the protection of data during storage | • System inputs recorded via log files  
• Access Control Lists defining users who have access and what level of access, following need to know and least privilege principles. |
| Measures for ensuring physical security of locations at which personal data are processed | • If utilizing a data center, ensure that it holds valid certifications attesting to its physical security, including SOC 2, ISO/IEC, or SAEE.  
• If not utilizing a data center, ensure that the appropriate level of physical security is in place following industry accepted frameworks including SOC or ISO/IEC. |
| Measures for ensuring events logging | • Procedures in place to regularly review logs.  
• Monitoring in place for log failure events.  
• Remote logging  
• Replication |
| Measures for ensuring system configuration, including default configuration | • Access Control Policy and Procedures  
• Baseline configuration identification  
• Configuration Planning and Management  
• Configuration Change Management  
• Configuration Status Accounting  
• Configuration Verification and Audits  
• Mobile device management |
| Measures for internal IT and IT security governance and management | • Dedicated and identified person to oversee the organization's information security and compliance program.  
• Information and network security personnel. |
| Measures for certification/assurance of processes and products | • Procedures in place for internal information security or quality management audits following industry accepted frameworks such as ISO/IEC, SOC, or SSAE 16. |
| Measures for ensuring data minimisation | • Restrict access to personal data to the parties involved in the processing in accordance with the “need to know” principle and according to the function behind the creation of differentiated access profiles.  
• Strict time limits for data retention and operational mechanisms that guarantee compliance (e.g. automatic deletion of data after predefined time period).  
• Technological barriers to the unauthorised linking of independent sources of data.  
• Limitation to the level of detail used in personal data processing: for example, through techniques such as differential privacy, k-anonymity, obfuscation and added noise measurement.  
• Deletion of metadata generated during certain processes that are not necessary for the pursued goal. |
| Measures for ensuring data quality | • Process for the exercise of data protection rights (right to amend and update information).  
• Data pipeline design to avoid duplicate data.  
• Enforcement of data integrity |
| Measures for ensuring limited data retention | • Automated controls to ensure the effectiveness and reliability of retention schedules.  
• Regular testing of automated controls to ensure the effectiveness and reliability of retention schedules. |
| Measures for ensuring accountability | • Assign responsibility to ensure end-user privacy throughout the product lifecycle and through applicable business processes.  
• Data protection impact assessments as an integral part of any new processing initiative. |
- Document all decisions that are adopted within the organization from a “privacy by design thinking” perspective.

| Measures for allowing data portability and ensuring erasure | • Documented processes in relation to the exercise by users of their privacy rights (e.g. right of erasure or right to data portability).  
• Use of open formats such as CSV, XML or JSON. |