Aditivo de Processamento de Dados MaxMind

(*Revisado em novembro de 2021)*

Este Aditivo ao Contrato de Processamento de Dados ("Aditivo") é parte integrante do Contrato de Licença do Usuário Final MaxMind, do Contrato de Licenciamento, do Contrato de Revendedor, do Contrato OEM ou Contrato de Licença do Usuário Final GeoLite2 ("Contrato") celebrado entre MaxMind, Inc. ("MaxMind") e o cliente definido neste instrumento como "você", "Licenciado" ou "Revendedor" ("você") e a celebração do Contrato é entendida pelas partes como celebração deste Aditivo e das Cláusulas Contratuais Padrão, conforme aplicável. A MaxMind e você são mencionados às vezes neste Aditivo individualmente como uma "parte" e conjuntamente, como as "partes".

Este Aditivo aplica-se ao tratamento de Dados Pessoais relacionadas ao uso dos Serviços por você. Exceto até o limite previsto de outra forma neste Aditivo, este Aditivo é regido pelos termos e condições do Contrato do qual o Aditivo é parte. Quaisquer termos definidos no Contrato, mas não definidos de outra forma neste instrumento têm os significados estipulados no Contrato. Para os fins deste Aditivo, o termo "usuários finais" inclui, sem limitação, seus clientes e seus respectivos usuários finais, conforme o caso. Ao celebrar este Contrato, você reconhece que leu este Aditivo e concorda em estar vinculado pelos seus termos. A MaxMind poderá revisar este Aditivo conforme necessário para tratar sobre alterações à Lei de Proteção de Dados Aplicável ou políticas da MaxMind, e essas mudanças serão vinculantes e entrarão em vigor em até (i) 30 (trinta) dias após a data de postagem do Aditivo revisado ou (ii) a data em que a MaxMind entregar aviso a você sobre o Aditivo revisado.

1. Definições.

a. "Lei de Proteção de Dados Aplicável" significa (i) Lei de Proteção de Dados Europeia (ii) a Lei de Privacidade do Consumidor da Califórnia de 2018, § 1798.100 e seguintes do Código Civil da Califórnia ("CCPA"); (iii) a Lei Geral de Proteção de Dados do Brasil, Lei nº 13.709 de 14 de agosto de 2018 ("LGPD"); (iv) a Lei de Proteção à Informação Pessoal ("PIPL") da República Popular da China ("PRC"); e (v) quaisquer outras leis, normas, regulamentos, diretrizes auto-regulatórias ou legislação de implementação sobre proteção de dados aplicáveis a qualquer disposição ou uso dos Serviços da parte.

b. "controlador(a)," "negócio," "processador(a)," "fornecedor(a) de serviço," "titular de dados," "consumidor," "processamento," "venda" e "autoridade supervisora" (ou quaisquer termos equivalentes) possuem cada um o significado definido nos termos da Lei de Proteção de Dados Aplicável.

c. "Informações Pessoais" significa informações que identifiquem, descrevam, se relacionem a um determinado consumidor, possam ser adequadamente capazes de serem associadas a um determinado consumidor ou adequadamente vinculadas, direta ou indiretamente, a um determinado consumidor, titular destas informações, ou casa ou são definidas como "informações identificáveis pessoalmente", "informações pessoais", "dados pessoais," ou termo similar nos termos da Lei de Proteção de Dados Aplicável.

d. "Lei de Proteção de Dados Europeia" significa (i) a Regulamentação (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção das pessoas naturais em relação ao processamento de dados pessoais e à livre movimentação desses dados e que revoga a Diretiva 95/46/EC (Regulamentação Da Proteção de Dados em Geral) ("GDPR"); (ii) com relação ao Reino Unido a Lei de Proteção de Dados do Reino Unido de 2018 e a GDPR conforme incluída na lei do Reino Unido em virtude da Cláusula 3 da (Retirada) da União Europeia do Reino Unido Lei 2018 (a "GDPR do RU"); (iii) a Diretiva sobre Privacidade Eletrônica da União Europeia (Diretiva 2002/58/EC); e (iv) a Lei Federal sobre Proteção de Dados da Suíça ("DPA da Suíça"), em cada caso conforme venha a ser complementada, atualizada ou revogada e substituída periodicamente.

e. "Transferência Restrita" significa: (i) nos casos em que a GDPR for aplicável, uma transferência de dados pessoais da Área Econômica Europeia para um país fora da Área Econômica Europeia que não está sujeito a uma decisão de adequação pela Comissão Europeia; (ii) nos casos em que a GDPR do Reino Unido for aplicável, uma transferência de dados pessoais do Reino Unido para qualquer outro país que não tem por base as regulamentações de adequação de acordo com a Cláusula 17ª da Lei sobre Proteção de Dados do Reino Unido de 2018; (iii) nos casos em que a DPA Suíça for aplicável, uma transferência de dados pessoais para um país fora da Suíça que está incluído na lista de jurisdições adequadas publicada pelo Conselheiro Federal de Proteção de Dados e Informações da Suíça, e (iv) nos casos em que a LGPD for aplicável, uma transferência de dados pessoais do Brasil para um país fora do Brasil que não fornece um nível adequado de proteção dentro do significado da LGPD.

f. "Cláusulas Contratuais Padrão" significa: (i) nos casos em que GDPR for aplicável, as cláusulas contratuais padrão anexadas à Decisão de Implementação 2021/914 de 4 de junho de 2021 sobre cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros de acordo com a Regulamentação (UE) 2016/679 do Parlamento Europeu e do Conselho ("SCCs da UE"); (ii) nos casos em que a GDPR do RU for aplicável, as cláusula sobre proteção de dados padrão aplicável adotadas de acordo com o Artigo 46(2)(c) ou (d) da GDPR do RU (Cláusulas Contratuais Padrão do Reino Unido –"CCPs do RU") e (iii) nos casos em que a DPA da Suíça for aplicável, as cláusulas padrão aplicáveis sobre proteção de dados emitidas, aprovadas ou reconhecidas pelo Conselheiro Federal de Proteção de Dados e Informações da Suíça (as "SCCs" da Suíça").

g. "Subprocessadoras" significa subcontratadas da MaxMind, que processam Informações Pessoais em nome da MaxMind em relação ao seu uso dos Serviços.

2. Processamento de Informações Pessoais Fornecidas por Você.

a. Reconhecimento. Você reconhece e concorda que a MaxMind processará Informações Pessoais que você fornecer à MaxMind em relação ao seu uso dos Serviços, incluindo-se nos Estados Unidos e em outros países em que a MaxMind ou suas prestadoras de serviços mantêm instalações. Para a lista atual de instalações que a MaxMind e suas prestadoras de serviços mantêm, é necessário solicitação por escrito para support@maxmind.com. Para evitar qualquer dúvida, a MaxMind não realiza qualquer atividade de tratamento de Informações Pessoais fornecidas por voce em conexão com serviços do GeoIP Databases ou GeoLite2 Databases e, portanto, a seção 6 deste Aditivo não se aplica aos serviços GeoIP Databases ou GeoLite2

Databases prestados pela MaxMind a você.

b. MaxMind como Processadora ou Fornecedora de Serviços. Sujeito à Cláusula 2(c), a MaxMind processa Informações Pessoais fornecidas por você em relação ao seu uso dos Serviços como um processador ou fornecedor de serviços em seu nome. Você é a controladora ou atividade comercial que determina quais Informações Pessoais são relevantes, e com base nessa análise, você instrui a MaxMind sobre como processar Informações Pessoais. Nos casos em que a MaxMind atua na qualidade de processadora ou prestadora de serviços em seu nome, as partes cumprirão as obrigações estipuladas na Seção 6 abaixo.

c. MaxMind na qualidade de Controladora ou Titular de Negócio. Em algumas circunstâncias, a MaxMind processa Informações Pessoais fornecidas por você na qualidade de controladora ou titular de negócio independente e você neste ato autoriza tal processamento de Informações Pessoais. Por exemplo, a MaxMind processa e agrega algumas das Informações Pessoais fornecidas por você a dados recebidos de outras fontes (incluindo-se outras licenciadas) a fim de melhorar os Serviços e fornecer a você e a outras licenciadas dados licenciados, informações mais precisas, informações robustas de pontuação de risco, e a capacidade de sinalizar atividade potencialmente fraudulenta, conforme aplicável. Mesmo depois que você parar de utilizar os Serviços, a MaxMind reterá as Informações Pessoais para as quais tiver base legal para tanto, incluindo-se para os fins dos próprios interesses legítimos da MaxMind de continuar a fornecer serviços para todas as licenciadas, respeitando suas obrigações legais, solucionando controvérsias, e fazendo valer seus contratos. Nos casos em que a MaxMind atua como uma controladora ou titular de negócio independente, você também será uma controladora ou negócio independente, e cada uma das partes será individualmente responsável pelo seu próprio processamento de Informações Pessoais e o cumprimento da Lei de Proteção de Dados Aplicável. Se o recebimento pela MaxMind de Informações Pessoais provenientes de você for considerado uma venda nos termos da CCPA, você garantirá que respeita suas obrigações na qualidade de negócio nos termos da CCPA.

d. Site na rede mundial de computadores. Se você fornecer Informações Pessoais por meio do site da internet da MaxMind (incluindo-se com relação a solicitações de correção), a MaxMind processará as Informações Pessoais de acordo com a política de privacidade da MaxMind disponível em https://www.maxmind.com/en/privacy-policy .

3. Processamento de Informações Pessoas Recebidas por Você. Você reconhece e concorda que poderá receber Informações Pessoais da MaxMind em relação ao seu uso dos Serviços, e que essas informações poderão estar relacionadas a assuntos ou consumidores de dados entre jurisdições (incluindo-se da Área Econômica Europeia, Suíça, Reino Unido e Brasil). Por exemplo, as Bases de Dados GeoIP ou Dados GeoIP licenciados para você poderão incluir Informações Pessoais. Nos casos em que você receber Informações Pessoais da MaxMind, você concorda que somente processará as Informações Pessoais para os fins estipulados no Contrato e de acordo com a Lei sobre Proteção de Dados Aplicável. A MaxMind e você, separadamente, são negócios ou controladoras independentes com relação às Informações Pessoais, e cada uma das partes será individualmente responsável pelo seu próprio processamento das Informações Pessoais e cumprimento da Lei de Proteção de Dados Aplicável. Se o seu recebimento de Informações Pessoais for considerado uma venda nos termos do CCPA e você receber uma solicitação de "Não Vender" de um consumidor (seja diretamente do consumidor ou repassada pela MaxMind), você

cessará prontamente qualquer uso ou venda das Informações Pessoais do consumidor aplicável no recebimento dessa solicitação por você. Você fornecerá à MaxMind toda assistência necessária para que a MaxMind examine qualquer questão de dados ou direitos do consumidor ou solicitações regulatórias nos termos da Lei de Proteção de Dados Aplicável.

4. Suas Obrigações. A MaxMind exige, e você neste ato declara e garante, que (i) forneceu quaisquer avisos e opções de escolha obrigatórios por lei, e tem uma base legal lícita para que você compartilhe, transmita, e processe Informações Pessoais da, com, para ou pela MaxMind; (ii) você respeitou todos os requisitos de transferência de dados de quaisquer jurisdições aplicáveis, e quaisquer transferências de dados de acordo com este Adendo não farão com que a MaxMind seja considerada como tendo descumprido a Lei de Proteção de Dados Aplicável; e (iii) quaisquer Informações Pessoais fornecidas por você não foram coletadas, armazenadas, ou transferidas para a MaxMind em violação de qualquer lei, regulamentação, ou obrigação contratual aplicável a você. Você concorda em manter uma política de privacidade que respeita a Lei de Proteção de Dados Aplicável e em divulgar suas práticas relacionadas ao seu uso dos Serviços e dados pessoais, e a não identificar expressamente a MaxMind em suas políticas a não ser que seja de outra forma exigido pela Lei de Proteção de Dados Aplicável. Você não fará quaisquer declarações nem prestará quaisquer garantias para seus usuários finais contrárias aos termos e condições no Contrato. Sem limitação da disposição anterior, se você fizer qualquer declaração ou prestar qualquer garantia a seus usuários finais contrárias aos termos e condições no Contrato, você será única e exclusivamente responsável por essa declaração ou garantia até o limite em que essa declaração ou garantia diferir daquelas no Contrato e a MaxMind não terá nenhuma responsabilidade por qualquer uma dessas declarações ou garantias. Entre a MaxMind e você, você é responsável por todas as ações e omissões de seus usuários finais em relação ao processamento de Informações Pessoais por eles, e você colaborará adequadamente com a MaxMind em relação a quaisquer atividades proibidas de qualquer usuário final em relação aos Serviços. Você notificará a MaxMind prontamente se ficar ciente de qualquer uma dessas atividades proibidas. Se as Cláusulas Padrão de Controladora para Controladora ou Cláusulas Padrão de Controladora para Processadora forem invalidadas por uma autoridade governamental competente, você trabalhará com a MaxMind para encontrar uma base legal alternativa para a transferência e processamento contínuo de Informações Pessoais em conformidade com a Lei de Proteção de Dados Aplicável, e você deixará de processar Informações Pessoais se nenhuma base for encontrada ou pactuada pela MaxMind.

5. Responsabilidade. Até o limite máximo previsto pela lei aplicável, a responsabilidade de cada parte está sujeita às isenções, limitações de responsabilidade, e obrigações de indenização no Contrato.

6. Termos Aplicáveis à MaxMind na qualidade de Processadora ou Fornecedora de Serviços.

a. Aplicação. Quando a MaxMind processa Informações Pessoais que você fornece na qualidade de processadora ou prestadora de serviço em seu nome (e não quando a MaxMind processa Informações Pessoais na qualidade de controladora ou titular do negócio), os termos desta Seção 6 são aplicáveis.

b. Instruções. Neste ato você instrui a MaxMind para processar Informações Pessoais

para as seguintes finalidades: (i) processamento de acordo com o Contrato; (ii) processamento iniciado pelos seus usuários finais no uso dos Serviços; e (iii) processamento para respeitar outras instruções adequadas documentadas fornecidas por você (por ex., via e-mail) no caso em que essas instruções são consistentes com os termos do Contrato. A MaxMind processará as Informações Pessoais apenas mediante instruções documentadas recebidas de você, a não ser se obrigada a agir de outra forma pela lei aplicável à qual a MaxMind está sujeita; nesse caso, a MaxMind informá-lo-á sobre aquele requisito legal antes de processar as Informações Pessoais, a não ser que a lei proíba essa divulgação com importantes alegações de interesse público. O Contrato constitui suas instruções documentadas completas e finais, e quaisquer instruções adicionais ou alternativas devem obrigatoriamente ser pactuadas separadamente entre as partes. Nos casos em que a MaxMind seguir suas instruções, você garantirá que suas instruções não farão com que a MaxMind viole quaisquer leis, normas, ou regulamentos aplicáveis ou obrigações contratuais.

c. Finalidade, Duração, Titulares dos Dados, e Tipos.

i. A finalidade do processamento é a execução dos Serviços para você de acordo com o Contrato.

ii. A duração do processamento será a duração do Contrato exceto quando de outra forma prevista em lei aplicável ou por obrigação legal, ou será a duração necessária para que a MaxMind proteja seus direitos ou aqueles de um terceiro.

iii. As categorias de titulares ou consumidores dos dados sobre os quais a MaxMind processa Informações Pessoais são determinadas e controladas por você, a seu único critério que poderão incluir, sem limitação, seus usuários finais.

iv. Os tipos de Informações Pessoais são determinados e controlados por você, a seu exclusivo critério, que poderão incluir, sem limitação, endereço de IP, endereço de e-mail, nome do usuário e senha, endereço de cobrança e de remessa, número de telefone, e informações sobre a transação.

d. CCPA. Para quaisquer Informações Pessoais sujeitas à CCPA [Lei de Proteção ao Consumidor da Califórnia], a MaxMind não: (i) venderá as Informações Pessoais; (ii) reterá, utilizará, ou divulgará as Informações Pessoais para qualquer finalidade que não seja para o fim específico de realizar os Serviços; (iii) reterá, utilizará ou divulgará as Informações Pessoais para um fim comercial que não seja o fornecimento dos Serviços; ou (iv) reterá, utilizará, ou divulgará as informações fora da relação comercial direta entre a MaxMind e você. A MaxMind certifica que entende estas restrições e as respeitará.

e. Subprocessadoras.

i. Neste ato você fornece à MaxMind uma autorização por escrito para contratar Subprocessadoras para auxiliarem no desempenho dos Serviços. A MaxMind celebrará um contrato por escrito com cada Subprocessadora contendo obrigações de proteção de dados não menos protetivas do que aquelas deste Adendo com respeito à proteção de Informações Pessoais

até o limite aplicável aos serviços fornecidos pela Subprocessadora. A MaxMind será responsável pelas ações e omissões de suas Subprocessadoras no mesmo limite em que a MaxMind seria responsável se realizasse os serviços de cada Subprocessadora diretamente nos termos do Contrato.

ii. A MaxMind disponibilizará a você uma lista atualizada de Subprocessadoras para os Serviços mediante solicitação por escrito. Você também poderá solicitar por escrito que a MaxMind notifique você sobre quaisquer novas Subprocessadoras. Se você fizer essa solicitação por escrito, a MaxMind fornecerá notificação de novas Subprocessadoras antes de autorizar quaisquer novas Subprocessadoras a processarem Informações Pessoais relacionadas ao fornecimento dos Serviços da MaxMind a você. Você poderá contestar o uso pela MaxMind de uma nova Subprocessadora mediante notificação por escrito à MaxMind prontamente no prazo de 10 (dez) dias úteis após o recebimento do aviso da MaxMind. Se você contestar uma nova Subprocessadora, a MaxMind utilizará esforços adequados para disponibilizar a você uma alteração nos Serviços ou recomendará uma mudança comercialmente adequada da sua configuração ou utilização dos Serviços para evitar o processamento de Informações Pessoais por novas Subprocessadoras contestadas sem onerá-lo de maneira inadequada. Se a MaxMind for incapaz de disponibilizar essa alteração num prazo adequado, que não excederá 30 (trinta) dias, você poderá rescindir os Serviços aplicáveis que não podem ser fornecidos pela MaxMind sem o uso da nova Subprocessadora que foi contestada mediante o fornecimento de aviso por escrito à MaxMind. A MaxMind reembolsará você por quaisquer taxas pré-pagas abrangendo o restante do prazo após a data de vigência da rescisão com respeito a esses Serviços rescindidos, sem a imposição de uma penalidade pela rescisão.

f. Solicitações. A MaxMind, até o limite legalmente permitido, notificará você se a MaxMind receber uma solicitação de um titular de dados ou consumidor para exercer seus direitos nos termos da Lei de Proteção de Dados Aplicável ("Solicitação"). Considerando a natureza do processamento, a MaxMind utilizará esforços comercialmente adequados para assisti-lo no cumprimento de sua obrigação de responder à Solicitação. Se permitido legalmente, você será responsável por quaisquer custos resultantes do fornecimento dessa assistência pela MaxMind. Você reconhece e concorda que a MaxMind poderá não ser capaz de atender a uma Solicitação nos casos em que se assim proceder ela descumpriria a legislação aplicável à MaxMind, interferiria na capacidade da MaxMind de cumprir obrigações legais ou proteger seus direitos ou direitos de um terceiro, ou impediria a MaxMind de continuar a processar Informações Pessoais se tiver um interesse legítimo em assim proceder.

g. Avaliações do Impacto da Proteção dos Dados. A MaxMind fornecerá a você colaboração e assistência adequadas conforme necessárias e apropriadas para que você cumpra suas obrigações nos termos da Lei de Proteção de Dados Aplicável para realizar uma avaliação do impacto da proteção de dados relacionado ao seu uso dos Serviços, se você de outra forma tiver acesso às informações relevantes, e se essas informações estejam disponíveis à MaxMind. A MaxMind fornecerá assistência adequada a você na colaboração com a Autoridade Competente ou consulta prévia a ela no desempenho de seus trabalhos relacionados à avaliação do impacto da proteção de dados, se exigido nos termos da Lei de Proteção de Dados Aplicável. Se permitido legalmente, você será responsável por quaisquer custos resultantes do fornecimento dessa assistência pela MaxMind.

h. Auditoria. Sujeito às disposições de confidencialidade estipuladas no Contrato, você poderá fazer uma solicitação por escrito em intervalos adequados para que a MaxMind

disponibilize a você uma cópia da auditoria mais recente até então da MaxMind com respeito às suas práticas de privacidade e proteção de dados, conforme o caso. Se após a entrega desse relatório pela MaxMind você desejar mais informações necessárias para demonstrar o cumprimento, pela MaxMind, de suas obrigações na qualidade de processadora ou fornecedora de serviços, então a MaxMind concorda mediante sua solicitação por escrito em submeter até o limite adequadamente possível, quaisquer instalações onde processa Informações Pessoais em seu nome para auditoria para verificar o cumprimento. Essa auditoria será realizada mediante sua solicitação adequada, com aviso adequado, em intervalos adequados (não maiores que uma vez por ano), durante o horário comercial normal, e sujeito às disposições de confidencialidade previstas no Contrato. Você é responsável por quaisquer despesas associadas à auditoria e reembolsará a MaxMind por elas. Você deve obrigatoriamente receber aprovação por escrito da MaxMind, a critério da própria MaxMind, antes de utilizar qualquer auditor terceiro, e esse terceiro auditor deve obrigatoriamente submeter-se a um dever de confidencialidade com respeito à auditoria.

i. Segurança. A MaxMind manterá medidas técnicas e organizacionais adequadas e apropriadas para a proteção da segurança, confidencialidade, e integridade de Informações Pessoais (incluindo-se proteção contra processamento não autorizado ou ilegal e contra destruição acidental ou ilegal, perda, ou alteração ou dano, divulgação não autorizada dessas Informações Pessoais ou acesso não autorizado a elas). A MaxMind regularmente monitora o cumprimento destas medidas. A MaxMind não diminuirá materialmente a segurança geral dos Serviços durante a prestação dos Serviços nos termos do Contrato. A MaxMind garante que todas as pessoas autorizadas para realizar o processamento comprometeram-se a manter sigilo ou estão sujeitas a uma adequada obrigação de confidencialidade prevista em lei.

j. Gerenciamento e Notificação de Incidente. A MaxMind mantém políticas e procedimentos de gerenciamento de incidentes de segurança e notificará você sem atraso injustificado quando tornar-se ciente da destruição acidental ou ilegal, perda, alteração, divulgação não autorizada das Informações Pessoais transmitidas, armazenadas ou de outra forma processadas pela MaxMind em seu nome (um "Incidente de Dados"). A MaxMind realizará esforços adequados para identificar a causa de um Incidente de Dados e providenciará o que a MaxMind considerar necessário e adequado a fim de corrigir a causa desse Incidente de Dados até o limite em que a remediação esteja sob controle adequado da MaxMind. A MaxMind não terá nenhuma responsabilidade perante você por Incidentes de Dados provocados por você ou seus usuários finais.

k. Devolução e Anulação. Mediante seu aviso por escrito, a MaxMind devolverá ou apagará Informações Pessoais processadas pela MaxMind em seu nome. A MaxMind poderá reter Informações Pessoais nos casos necessários para que a MaxMind cumpra a lei aplicável ou obrigações legais, ou para proteger seus direitos ou direitos de um terceiro.

7. Transferências Internacionais de Informações Pessoais

a. As partes concordam que em caso de qualquer transferência de Informações Pessoais de você (na qualidade de "exportador de dados") para a MaxMind (na qualidade de "importadora de dados") isto significa uma Transferência Restrita e as Leis de Proteção de Dados Aplicáveis exigem que sejam colocadas salvaguardas adequadas, que essa transferência esteja sujeita a Cláusulas Contratuais Padrão adequadas, que serão consideradas incorporadas a este Adendo e formam uma parte dele, como se segue:

i. Em relação a transferências de Informações Pessoais que estejam protegidas pela Lei Geral de Proteção de Dados da União Europeia (LGPD da UE) e processadas de acordo com a Cláusula 2(b) deste Adendo, as Cláusulas Contratuais Padrão da União Europeia (EU SCCs, *na sigla em inglês*) serão aplicáveis, de acordo com o seguinte:

A. O Módulo Dois ou o Módulo Três serão aplicáveis (conforme o caso);

B. na Cláusula 7, a cláusula opcional de "*docking*" será aplicável;

C. na Cláusula 9, a Opção 2 será aplicável, e o prazo para aviso prévio de alterações da Subprocessadoras será conforme estipulado na Cláusula 6(e)(ii) deste Adendo;

D. na Cláusula 11, o idioma opcional não será aplicável;

E. na Cláusula 17, a Opção 1 será aplicável e as EU SCCs serão regidas pela lei irlandesa;

F. na Cláusula 18(b), as controvérsias serão solucionadas perante os tribunais da Irlanda;

G. O Anexo I das EU SCCS será considerado preenchido com as informações estipuladas no Anexo 1.2 a este Adendo; e

H. Sujeito à cláusula 6(i) deste DPA, o Anexo II das EU SCCS será considerado preenchido com as informações estipuladas no Anexo 3 a este Adendo; e

ii. Em relação a transferências de informações pessoais protegidas pela Lei Geral de Proteção de Dados da União Europeia (LGPD da UE) e processadas de acordo com a Cláusula 2(c) deste DPA (Adendo), as Cláusulas Contratuais Padrão da União Europeia (EU SCCs) serão aplicáveis, completadas conforme a seguir:

A. O Módulo Um será aplicável;

B. na Cláusula 7, a cláusula opcional de "*docking*" será aplicável;

C. na Cláusula 11, o idioma opcional não será aplicável;

D. na Cláusula 17, a Opção 1 será aplicável e as EU SCCs serão regidas pela lei irlandesa;

E. na Cláusula 18(b), as controvérsias serão solucionadas perante os tribunais da Irlanda;

F. O Anexo I das EU SCCS será considerado preenchido com as informações estipuladas no Anexo 1.2 a este Adendo; e

G. Sujeito ao idioma estipulado na Cláusula 6(i) deste Adendo, o Anexo II das EU SCCs será considerado preenchido com as informações estipuladas no Anexo 3 a este Adendo;

iii. Em relação a transferências de dados pessoais que estejam protegidos pela Lei Geral de Proteção de Dados do Reino Unido (LGPD do Reino Unido) ou pela DPA ou LGPD da Suíça, as Cláusulas Contratuais Padrão da União Europeia (EU SCCs) também serão aplicáveis de acordo com os parágrafos (i) e (ii) acima, com as seguintes modificações:

A. as menções a "Regulamentação (EU) 2016/679" serão interpretadas como menções à GDPR do RU ou à DPA ou LGPD da Suíça (conforme o caso);

B. as menções a Artigos da "Regulamentação (EU) 2016/679" específicos serão substituídas pelo artigo ou cláusula equivalente da GDPR do RU ou à DPA ou LGPD da Suíça (conforme o caso);

C. as menções a "UE", "União", "Estado Membro" e "lei do Estado Membro" serão substituídas por menções ao "RU", ou à "Suíça" ou ao "Brasil", ou à lei do RU", ou à "lei da Suíça" ou à lei brasileira" (conforme o caso);

D. o termo "estado membro" não será interpretado de uma maneira a excluir os titulares dos dados no RU ou na Suíça ou no Brasil da possibilidade de propor ação por seus direitos em seu local de residência habitual (isto é, o Reino Unido ou a Suíça ou o Brasil);

E. A Cláusula 13(a) e a Parte C do Anexo I não são utilizadas e a "autoridade supervisora competente" é o Conselheiro de Informações do Reino Unido ou o Conselheiro Federal de Informações sobre Proteção de Dados da Suíça ou a Autoridade de Proteção de Dados do Brasil (conforme o caso).

F. referências à "autoridade supervisora competente" e aos "juízos competentes" serão substituídas por referências ao "Conselheiro de Informações" e aos "juízos da Inglaterra e País de Gales" ou ao "Conselheiro Federal de Informações sobre Proteção de Dados da Suíça" e aos "juízos aplicáveis da Suíça" ou à "Autoridade de Proteção de Dados do Brasil" e aos "juízos do Brasil" (conforme o caso);

G. na Cláusula 17, as Cláusulas Contratuais Padrão serão regidas pelas leis da Inglaterra e País de Gales ou Suíça ou Brasil (conforme o caso); e

H. com respeito a transferências às quais a GDPR do Reino Unido é aplicável, a Cláusula 18 será alterada para estipular que "Qualquer controvérsia resultante destas Cláusulas será dirimida pelos tribunais da Inglaterra e País de Gales. Um titular de dados poderá ingressar com medidas judiciais contra a exportadora e/ou importadora de dados perante os tribunais de qualquer país do RU. As Partes concordam em estarem sujeitas à jurisdição desses tribunais", e com respeito a transferências às quais o DPA suíço é

aplicável, a Cláusula 18(b) estipulará que as controvérsias serão dirimidas perante os juízos aplicáveis da Suíça,

a não ser que as Cláusulas Contratuais Padrão da UE, implementadas conforme descrito acima, não podem ser utilizadas para transferir legalmente esses dados pessoais em cumprimento ao quanto estipulado na GDPR do RU ou DPA da Suíça caso em que as Cláusulas Contratuais Padrão do Reino Unido ou da Suíça (conforme o caso) serão, ao invés disso, incorporadas mediante menção e constituirão uma parte integrante deste Adendo e serão aplicáveis a essas transferências. Se este for o caso, os Anexos ou Apêndices relevantes das Cláusulas Contratuais Padrão do RU ou da Suíça serão preenchidos utilizando as informações contidas nos Anexos 1.1, 1.2 e 3 do Adendo (conforme o caso);

b. As partes concordam que em caso de qualquer transferência de Informações Pessoais da MaxMind (na qualidade de "exportadora de dados") para você (na qualidade de "importador de dados") isto significa uma Transferência Restrita e as Leis sobre Proteção de Dados Aplicáveis exigem que sejam colocadas salvaguardas adequadas, que essa transferência esteja sujeita a Cláusulas Contratuais Padrão adequadas, que serão consideradas incorporadas a este Adendo e formam uma parte dele, como se segue:

i. Em relação a transferências de dados pessoais que estejam protegidos pela Lei Geral de Proteção de Dados da União Europeia (LGPD da UE) e processadas de acordo com a Cláusula 3 deste Adendo, as Cláusulas Contratuais Padrão da União Europeia (EU SCCs) serão aplicáveis, completadas conforme a seguir:

A. O Módulo Um será aplicável;

B. na Cláusula 7, a cláusula opcional de *docking* será aplicável;

C. na Cláusula 11, o idioma opcional não será aplicável;

D. na Cláusula 17, a Opção 1 será aplicável e as EU SCCs serão regidas pela lei irlandesa;

E. na Cláusula 18(b), as controvérsias serão solucionadas perante os tribunais da Irlanda;

F. O Anexo I das Cláusulas Contratuais Padrão da União Europeia (EU SCCs) será considerado preenchido com as informações estipuladas no Anexo 4 a este Adendo; e

G. O Anexo II das Cláusulas Contratuais Padrão da União Europeia (EU SCCs) será considerado preenchido com as informações estipuladas no Anexo 5 a este Adendo;

ii. Em relação a transferências de informações pessoais que estejam protegidas pela Lei Geral de Proteção de Dados do Reino Unido (LGPD do Reino Unido) ou pela DPA ou LGPD da Suíça, as Cláusulas Contratuais Padrão da União Europeia (EU SCCs) também serão aplicáveis de acordo com o parágrafo (i) acima, sujeito às mesmas modificações conforme estão

descritas na Cláusula 7(a)(iii); a não ser que as Cláusulas Contratuais Padrão da União Europeia, implementadas conforme descrito nesta Cláusula 7(b)(ii), não podem ser utilizadas para transferir legalmente essas Informações Pessoais em cumprimento à GDPR do RU ou ao DPA da Suíça caso em que as Cláusulas Contratuais Padrão do Reino Unido ou as Cláusulas Contratuais Padrão da Suíça (conforme o caso) serão, ao invés disso, incorporadas mediante menção e constituirão uma parte integrante deste Adendo e serão aplicáveis a essas transferências. Se este for o caso, os Anexos ou Apêndices relevantes das Cláusulas Contratuais Padrão do RU ou da Suíça serão preenchidos utilizando as informações contidas nos Anexos 4 e 5 do Adendo (conforme o caso);

c. Não é intenção de nenhuma das partes contradizer ou restringir qualquer uma das disposições estipuladas nas Cláusulas Contratuais Padrão e, consequentemente, se e até o limite em que as Cláusulas Contratuais Padrão estiverem em conflito com qualquer dispositivo do Contrato (incluindo-se este Adendo) as Cláusulas Contratuais Padrão prevalecem até o limite desse conflito.

d. As partes concordam que em caso de qualquer transferência de Informações Pessoais de você para MaxMind estar sujeita à PIPL ou a outras leis ou padrões aplicáveis na PRC, que você buscará obter consentimento em separado e/ou cumprir com demais dispositivos da PIPL e/ou outras leis ou padrões da PRC aplicáveis. No limite em que uma transferência de Informações Pessoais de você para a MaxMind esteja sujeita à PIPL, a finalidade, o período e o método de processamento serão aqueles definidos no Anexo 1.1 e 1.2 e as medidas de segurança e proteção a serem adotadas pela MaxMind serão aquelas definidas no Anexo 3.

8. Assinatura e Vigência. As partes concordam que este Adendo (e as Cláusulas Contratuais Padrão, conforme o caso), estão mencionados neste Contrato e constituem uma parte integrante do Contrato e a assinatura do Contrato será considerada como sendo uma inclusão da assinatura deste Adendo e das Cláusulas Contratuais Padrão (conforme o caso), até o limite exigido pela lei aplicável.

Anexo 1.1

Descrição do Processamento / da Transferência

Módulos 2 e 3 (transferências da controladora/processadora para a processadora)

A. LISTA DAS PARTES

Exportadora(s) de Dados:

1.	Nome:	Parte identificada como "você" no Adendo
	Endereço	O endereço para avisos fornecido por você à MaxMind
	Nome, cargo e detalhes da pessoa de contato:	A pessoa de contato, cargo dessa pessoa e detalhes de contato fornecidos por você à MaxMind.
	Atividades relevantes para os dados transferidos nos termos destas Cláusulas:	Fornecimento de dados com a finalidade de utilizar os Serviços.
	Função:	Controladora/ Processadora

Importadora de dados:

1.	Nome:	MaxMind, Inc.
	Endereço:	14 Spring Street, Suite #3, Waltham, Massachussetts 02451, Estados Unidos
	Nome, cargo e detalhes de contato da pessoa de contato:	MaxMind, Inc. Departamento Jurídico e-mail: legal@maxmind.com
	Atividades relevantes para os dados transferidos nos termos destas Cláusulas:	Fornecimento dos Serviços descritos no Contrato. Por exemplo: • Para minFraud: Fornecer análise de risco e fraude e dados relativos à inteligência de Endereços de IP. • Para Serviço de Precisão GeoIP2 e Serviço de Internet GeoLite: Fornecimento de dados relativos a Endereço(s) de IP. • Para o Serviço de Precisão GeoIP2, Serviço minFraud e Serviço da Internet GeoLite2: Fornecimento de suporte técnico para os Serviços e melhoria dos Serviços, logging e backup.
	Função:	Processadora

B. DESCRIÇÃO DA TRANSFERÊNCIA

Categorias de titulares de dados cujos dados pessoais são transferidos:	Usuários finais da exportadora de dados e aqueles de seus clientes, parceiros comerciais, e outros terceiros.
Categorias de dados pessoais transferidos:	Os dados pessoais transferidos têm base nos produtos ou serviços utilizados de acordo com o Contrato, que poderão incluir, sem limitação, as seguintes categorias de dados pessoais: • Para o Serviço de Precisão GeoIP2 e Serviço da Internet GeoLite2: Endereços de IP • Para o Serviço minFraud: Endereços de IP, rede, nível de código postal ou nível menos preciso de dados de geolocalização, nome e endereço de e-mail.
Dados sensíveis transferidos (se aplicável) e restrições ou salvaguardas aplicadas que levam em consideração integralmente a natureza dos dados e os riscos envolvidos, tais como, por exemplo, rigorosa limitação de finalidade, restrições de acesso (incluindo-se acesso apenas para o quadro de pessoal que tenha recebido treinamento especializado), mantendo um registro de acesso aos dados, restrições para transferências subsequentes ou medidas de segurança adicionais:	Quaisquer dados sensíveis não serão transferidos.
A frequência da transferência (por ex., se os dados são transferidos numa base pontual ou de maneira contínua):	Contínua – os dados serão transferidos periodicamente durante o prazo do Contrato.
Natureza do processamento:	Os dados pessoais transferidos estarão sujeitos às seguintes atividades básicas de processamento (conforme o caso): ● Fornecimento de análise de risco e fraude e serviços e produtos de inteligência de Endereços de IP. ● Fornecimento de suporte técnico para os serviços e produtos da MaxMind e melhoria desses serviços e produtos. ● Fornecimento de dados licenciados. ● Logging e backup.

Finalidade(s) da transferência de dados e processamentos adicionais:	Para as finalidades com base nos Serviços utilizados de acordo com o Contrato, incluindo-se o fornecimento de serviços de Geolocalização de IP, detecção de fraudes e serviços relacionados.
O período pelo qual os dados pessoais estarão retidos, ou, se isso não for possível, os critérios utilizados para estabelecer esse período:	Os dados pessoais são apagados no prazo de 30 dias para dados apresentados para o Serviço de Precisão GeoIP, no prazo de 4 meses para dados apresentados ao Serviço minFraud que têm uma pontuação baixa de risco, conforme estipulado pela MaxMind, e no prazo de 15 meses para dados apresentados ao Serviço minFraud que têm uma pontuação alta de risco conforme estipulado pela MaxMind.
Para transferências para (sub-) processadoras, especificar também o assunto, a natureza e duração do processamento:	A Google, Inc. hospeda a infraestrutura do centro de dados da MaxMind pelo período em que a MaxMind retém os dados. A Cloudflare, Inc. fornece DNS e segurança para os Serviços e o prazo do processamento da Cloudfare para cada solicitação ou interação com o site da MaxMind na internet dura menos de 1(um) segundo.

C. AUTORIDADE SUPERVISORA COMPETENTE

Identificar a(s) autoridade(s) supervisora(s) competente(s) de acordo com a Cláusula 13 das SCCSs da UE (se aplicável)	Para transferências em que a GDPR for aplicável – a autoridade supervisora competente será determinada de acordo com os critérios estipulados na Cláusula 13 das SCCs da UE, desde que se a exportadora de dados não está estabelecida num Estado-Membro da UE e não indicar um representante, a Autoridade Supervisora Irlandesa atuará como a autoridade supervisora competente. Para transferências em que a LGPD for aplicável a autoridade supervisora competente é a Autoridade de Proteção de Dados do Brasil. Para transferências em que a LGPD do RU for aplicável a autoridade supervisora competente é o Escritório do Conselheiro de Informações do RU. Para transferências em que a DPA suíça for aplicável, a autoridade supervisora

	competente é o Conselheiro Federal de Informações e Proteção de Dados da Suíça.

Anexo 1.2

Descrição do Processamento / Transferência

Módulo 1 (transferências de controladora para controladora)

A. LISTA DAS PARTES

Exportadora(s) de Dados:

1.	Nome:	Parte identificada como "Você" no Adendo
	Endereço	O endereço para avisos fornecido por você à MaxMind.
	Nome, cargo e detalhes de contato da pessoa de contato:	A pessoa de contato, cargo dessa pessoa e detalhes de contato fornecidos por você à MaxMind.
	Atividades relevantes para os dados transferidos nos termos destas Cláusulas:	Fornecimento de dados com a finalidade de utilizar os Serviços e permitir a melhoria dos serviços.
	Função:	Controladora

Importadora de dados:

1.	Nome:	MaxMind, Inc.,
	Endereço:	14 Spring Street, Suite #3, Waltham, Massachussetts 02451, Estados Unidos
	Nome, cargo e detalhes de contato da pessoa de contato:	MaxMind, Inc. Departamento Jurídico e-mail: legal@maxmind.com
	Atividades relevantes para os dados transferidos nos termos destas Cláusulas:	Melhoria dos Serviços
	Função:	Controladora

B. DESCRIÇÃO DA TRANSFERÊNCIA

Categoria de titulares de dados cujos dados pessoais são transferidos:	Usuários finais da exportadora de dados e aqueles de seus clientes, parceiros comerciais, e outros terceiros.
Categorias de dados pessoais transferidos:	Os dados pessoais transferidos têm base nos produtos ou serviços utilizados de acordo com o Contrato, que poderão incluir, sem limitação, as seguintes categorias de dados pessoais:

	• Para o Serviço de Precisão GeoIP2 e Serviço da Internet GeoLite2: Endereços de IP • Para o Serviço minFraud: As categorias de dados pessoais transferidos poderão incluir, mas sem limitação, endereço de IP, rede, nível de código postal ou nível menos preciso de dados de geolocalização, nome e endereço de e-mail.
Dados sensíveis transferidos (se aplicável) e restrições ou salvaguardas aplicadas que levam em consideração integralmente a natureza dos dados e os riscos envolvidos, tais como, por exemplo, rigorosa limitação de finalidade, restrições de acesso (incluindo-se acesso apenas para o quadro de pessoal que tenha efetuado treino especializado), mantendo um registro de acesso aos dados, restrições para transferências subsequentes ou medidas de segurança adicionais:	Quaisquer dados sensíveis não serão transferidos.
A frequência da transferência (por ex., se os dados são transferidos de forma pontual ou de maneira contínua):	Contínua – os dados serão transferidos periodicamente durante o prazo do Contrato.
Natureza do processamento:	A MaxMind processa e agrega dados pessoais fornecidos por você a dados recebidos de outras fontes (incluindo-se outras licenciadas) a fim de melhorar os Serviços e fornecer a você e a outras licenciadas dados licenciados, informações mais precisas, informações robustas de pontuação de risco, e a capacidade de sinalizar atividade potencialmente fraudulenta.
Finalidade(s) da transferência de dados e processamentos adicionais:	Com a finalidade de melhorar os Serviços.
O período pelo qual os dados pessoais estarão retidos, ou, se isso não for possível, os critérios utilizados para estabelecer esse período:	Os dados pessoais são apagados no prazo de 30 dias para dados apresentados para o Serviço de Precisão GeoIP, no prazo de 4 meses para dados apresentados para o Serviço minFraud estipulado pela MaxMind que têm uma pontuação baixa de risco, e no prazo de 15 meses para dados apresentados ao Serviço minFraud estipulado pela MaxMind que têm uma pontuação alta de risco.
Para transferências para (sub-) processadoras, especificar também o assunto, a natureza e duração do	A Google, Inc. hospeda a infraestrutura do centro de dados da MaxMind pelo período em que a MaxMind retém os dados.

processamento:	A Cloudflare, Inc fornece DNS e segurança para os Serviços e o prazo do processamento da Cloudfare para cada solicitação ou interação com o site da MaxMind na internet dura menos de 1(um) segundo.

C. AUTORIDADE SUPERVISORA COMPETENTE

Identificar a(s) autoridade(s) supervisora(s) competente(s) de acordo com a Cláusula 13 das SCCSs da UE (se aplicável)	Para transferências em que a GDPR for aplicável – a autoridade supervisora competente será determinada de acordo com os critérios estipulados na Cláusula 13 das SCCs da UE, desde que se a exportadora de dados não estiver estabelecida num Estado-Membro da UE e não indicar um representante, a Autoridade Supervisora Irlandesa atuará como a autoridade supervisora competente. Para transferências em que a LGPD for aplicável a autoridade supervisora competente é a Autoridade de Proteção de Dados do Brasil. Para transferências em que a LGPD do RU for aplicável, a autoridade supervisora competente é o Escritório do Conselheiro de Informações do RU. Para transferências em que a DPA suíça for aplicável, a autoridade supervisora competente é o Conselheiro Federal de Informações e Proteção de Dados da Suíça.

Anexo 2
Subprocessadoras

Subprocessadora	Breve Descrição do Processamento	Localizações do Centro de Dados
Cloudflare, Inc.	Serviços de Segurança e DNS para tráfego na internet transmitido dos Serviços e para estes.	Global https://www.cloudflare.com/network/
Google Inc.	Armazenamento na Google Cloud	Iowa, EUA
Google Inc.	Plataforma da Google Cloud – Fornecedora de infraestrutura em nuvem	Iowa, EUA Oregon, EUA N. Virginia, EUA Reino Unido Cingapura

Anexo 3

Medidas Técnicas e Organizacionais Mínimas

1. Gerenciamento de Risco

- Uma avaliação de risco contínua da Segurança das Informações é realizada cobrindo as instalações e bens informacionais da MaxMind.
- A avaliação de risco é conduzida utilizando-se uma metodologia padrão da indústria (com base na ISO 27001) para auxiliar na identificação, medição, e tratamento de riscos conhecidos.
- Os resultados da avaliação de riscos e sugestões de mitigação de riscos são compartilhados com a gestão sênior.
- Os resultados da avaliação de riscos especificam as alterações propostas para sistemas, processos, políticas, ou ferramentas, a fim de reduzir vulnerabilidades e ameaças à segurança.
- Um Diretor de Proteção de Dados (DPD) que é independente, examina regularmente os riscos e controles de proteção de dados.

2. Política de Segurança.

- As políticas, incluindo-se aquelas relacionadas à privacidade, segurança e uso aceitável dos dados, são avaliadas e aprovadas pela gestão sênior da MaxMind. As políticas são documentadas e publicadas para todo o pessoal relevante**.**
- Os empregados e terceiros contratados devem obrigatoriamente cumprir as políticas da MaxMind relevantes para o escopo de seu trabalho.
- Os novos empregados recebem treinamento sobre obrigações de confidencialidade, segurança de informações, compliance, e proteção de dados.
- Os empregados recebem atualizações de treinamento regulares, que abrangem as políticas e expectativas da Segurança das Informações da MaxMind.
- Se necessário, as políticas são suportadas por procedimentos, padrões e diretrizes associadas.
- As políticas de Segurança das Informações são atualizadas, conforme necessário, para refletirem as alterações dos objetivos comerciais ou risco.
- A administração sênior efetua uma análise anual de todas as políticas de Segurança das Informações.
- As políticas de Segurança das Informações são armazenadas, mantidas, atualizadas, e publicadas num local on-line centralizado.
- O Sistema de Gestão da Segurança das Informações da MaxMind contém cláusulas sobre requisitos de senhas, uso da Internet, segurança dos computadores, confidencialidade, proteção dos dados do cliente, e a proteção de dados da MaxMind.

3. Organização da Segurança das Informações.

- A governança da Segurança das Informações e o cumprimento da proteção de dados para a MaxMind são de responsabilidade do Diretor de Operações da MaxMind.
- A MaxMind constituiu um time de Segurança das Informações, com responsabilidades de segurança compartilhadas entre diversas unidades de negócio.
- Acordos de confidencialidade e não-divulgação são exigidos no compartilhamento de informações sensíveis, de propriedade exclusiva, pessoais ou informações confidenciais de outra forma entre a MaxMind e um terceiro.
- Um processo formal está implementado para administrar terceiros com acesso a dados organizacionais, sistemas de computadores, ou centros de dados. Todos esses terceiros comprometem-se contratualmente a manter a confidencialidade de todas as informações confidenciais.

4. Gerenciamento de Bens.

- A MaxMind transfere a propriedade para todos os bens informacionais.
- A MaxMind mantém uma política de classificação de bens informacionais e classifica esses bens em termos de valor, requisitos legais, sensibilidade, e criticalidade para a organização.
- Computadores e laptops utilizam criptografia total de disco.
- A MaxMind mantém uma política de disponibilidade e destruição de dados que abrange o descarte de bens eletrônicos e mídia associada.

5. Segurança das Informações sobre Recursos Humanos.

- As responsabilidades e atribuições para empregados estão definidas e documentadas.
- A MaxMind realiza uma triagem do histórico de novas contratações incluindo-se histórico de empregos, referências e verificações de registros criminais (sujeito à legislação local).
- A MaxMind exige que todos os novos empregados assinem contratos de trabalho, que incluem compromissos abrangentes de confidencialidade e não divulgação.
- A MaxMind mantém um programa de treinamento e conscientização da segurança das informações que inclui o treinamento de novas contratações.
- A conscientização da Segurança das Informações é aprimorada por meio de comunicações regulares mediante e-mails que abrangem toda a empresa, conforme necessário.
- A organização mantém registros de presença para quaisquer sessões formais de treinamento de conscientização da segurança.
- O departamento de Recursos Humanos notifica o time de Operações sobre eventuais alterações na situação do contrato de trabalho e rescisão contratual.

- A MaxMind mantém um procedimento documentado para alterações na situação do contrato de trabalho e rescisão contratual (incluindo-se notificação, modificação do acesso, e arrecadação de bens).
- Os novos fornecedores de serviço terceirizados cujos serviços envolvem o acesso a quaisquer informações confidenciais devem obrigatória e contratualmente concordar com os compromissos de privacidade e segurança dos dados compatíveis com o acesso e manuseio de informações confidenciais.
- A Política de Privacidade da MaxMind inclui dispositivos relacionados ao compartilhamento de dados com terceiros fornecedores de serviços e suas obrigações de manter a confidencialidade desses dados.

6. Segurança Ambiental e Física.

- Os controles de segurança física em todos os centros de dados utilizados pela MaxMind, no fornecimento do Serviço, incluem múltiplas camadas de segurança física incluindo-se identificação biométrica, detectores de metal, entrada supervisionada, times de segurança 24/7/365 no local, sistemas de CCTV, barreiras de veículos, e sistemas de detecção de intrusão com base em laser.
- O acesso aos centros de dados está limitado apenas a empregados ou contratados autorizados.
- Há controles instalados para proteção contra danos ambientais em todos os centros de dados.
- Todas as instalações dos centros de dados foram atestadas com êxito pela SSAE 16, SOC 2 tipo 2, ISO 27001, ou requisitos similares.

7. Gestão de Comunicações e Operações.

- A operação dos sistemas e aplicativos que dão suporte aos Serviços está sujeita aos procedimentos de operação documentados.
- O time do *Site Reliability Engineer* (SRE) [Engenheiro de Confiabilidade do Site] mantém as configurações padronizadas do servidor.
- Ambientes separados são mantidos para permitir a testagem de alterações.
- O acesso de terceiros aos sistemas da MaxMind é auditado regularmente.
- A organização mantém procedimentos de *backup* documentados. Backups completos são realizados regularmente para todas as bases de dados de produção. Os *backups* de dados são transferidos para um local remoto de acordo com uma programação regular e estão armazenados de modo criptografado.
- Todos os sistemas e dispositivos de rede estão sincronizados com uma fonte horária precisa por meio do "Protocolo de Tempo da Rede" (NTP, *na sigla em inglês*).

- Todas as ferramentas de alerta de evento de alta prioridade tornam-se notificações para os times de resposta a incidentes disponíveis 24x7, fornecendo alertas ao time de SRE, conforme necessário.
- Controles de segurança de rede que preveem o uso de tecnologia de firewall nativo da nuvem, Nuvem Privada Virtual (NPV), arquitetura com limites de confiança restritos, e sistemas de detecção de intrusão e outros procedimentos de correlação de tráfego e evento projetados para proteger os sistemas contra intrusão e limitar o escopo de qualquer ataque efetivo.

8. Controles do Acesso.

- A MaxMind mantém uma política de "Uso Aceitável" que delineia os requisitos para o uso de IDs de usuário e senhas.
- A organização publica e mantém uma norma de gerenciamento de senhas. Os controles de senhas são destinados a gerenciar e controlar a força da senha, e sua utilização, incluindo-se a proibição de que usuários compartilhem senhas.
- Práticas eficazes de autenticação (por ex., senhas SSH, restrições baseadas em IP, 2FA [*autenticação de 2 fatores*]) são utilizadas para controlar o acesso aos ambientes de produção e desenvolvimento.
- O acesso direito à conta "raiz" em todos os servidores da produção está restrito ao pessoal da Administração do Sistema e Engenharia de Softwares considerado necessário.
- Todos os controles de acesso têm por base os princípios "negado por padrão", "privilégios mínimos" e "acesso por necessidade de ter conhecimento". Funções diferentes, incluindo-se acesso limitado e administrativo, são utilizadas no ambiente.
- Auditoria do Sistema ou o evento de logar no Sistema e procedimentos de monitoramento relacionados para registrar proativamente o acesso do usuário e atividade do sistema para exame de rotina.
- Mediante aviso de rescisão, o acesso total do usuário é removido. Todo acesso crítico ao sistema é removido imediatamente mediante notificação.

9. Aquisição, Desenvolvimento, e Manutenção dos Sistemas de Informações.

- As características do produto são administradas por meio de um processo formalizado de gerenciamento do produto. Os requisitos de segurança são discutidos e formulados durante as discussões sobre escopo e projeto.
- A MaxMind mantém um Departamento de Garantia de Qualidade (GQ) dedicado a examinar e testar a funcionalidade e estabilidade do aplicativo.
- O código fonte do aplicativo é armazenado num repositório central. O acesso ao código fonte é restrito a indivíduos autorizados.
- As alterações aos softwares da MaxMind são testadas antes da implementação da produção. Os processos de implementação incluem testagem por unidade no ambiente da fonte, bem

como teste de integração e funcional dentro de um ambiente de teste antes da implementação na produção.

- Procedimentos de gerenciamento de alterações e mecanismos de rastreamento destinados a testar, aprovar e monitorar todas as alterações nos bens de tecnologia e informação da MaxMind.
- Avaliação da vulnerabilidade, gestão de (patch) lotes, e tecnologias de proteção contra ameaças e procedimentos de monitoramento programados destinados a identificar, avaliar, mitigar e proteger contra ameaças à segurança identificadas, vírus e outros códigos mal-intencionados.
- Programa Gerenciamento de Vendedor Formal, incluindo-se exames de segurança do vendedor para vendedores essenciais para assegurar o cumprimento das Políticas de Segurança das Informações da MaxMind.

10. Gestão de Incidente de Segurança das Informações.

- A MaxMind mantém um processo de resposta a incidentes.
- A MaxMind mantém um plano de resposta a incidentes que é testado regularmente. O plano aborda procedimentos específicos de respostas a incidentes, procedimentos de backup de dados, atribuições e responsabilidades, comunicação com o cliente, estratégias de contato, e fluxo de informações jurídicas.
- Os procedimentos de gerenciamento de incidentes são destinados a permitir que a MaxMind investigue, enfrente, atenue e notifique os eventos relacionados aos bens de tecnologia e informação da MaxMind.
- O plano de resposta a incidentes é objeto de exercício regular, pelo menos uma vez por ano.

11. Gestão de Continuidade do Negócio.

- Procedimentos de resiliência/continuidade do Negócio, conforme o caso, destinados a manter o serviço e/ou recuperação de situações ou desastres de situações emergenciais previsíveis.
- Para redundância, a MaxMind utiliza arquiteturas de replicação de base de dados.
- Os backups de base de dados são armazenados em discos locais em centros de dados, bem como copiados para locais de armazenagem remotos.
- A MaxMind implementou infraestrutura redundante do centro de dados para melhor apoiar a alta disponibilidade ao sistema como um todo. Cada camada de serviços-chave inclui componentes redundantes que diminuem o impacto de falhas previsíveis tais como problemas de hardware, e também permite a capacidade de expansão conforme os dados do cliente e seu uso aumentem.

12. Características de Segurança do Aplicativo da MaxMind.

- Para o acesso aos serviços da MaxMind é necessária uma senha de licença exclusiva, e o acesso ao portal de conta de um cliente exige um login e senha. A MaxMind apoia e incentiva o uso de HTTPS para todas as comunicações com nosso site da internet e serviços.

- A comunicação com os serviços da MaxMind utiliza protocolos criptográficos tais como TLS para proteger as informações em trânsito em redes públicas. No limite da rede, gestão bot, firewalls de aplicativos da internet, e proteção DDoS são utilizados para filtrar ataques. Dentro da rede interna, os aplicativos seguem um modelo de camadas múltiplas que fornece a capacidade de aplicar controles de segurança entre cada camada.

- Os controles de segurança de dados que incluem segregação lógica de dados, acesso restrito (por exemplo, com base no cargo) e monitoramento e, se for aplicável, utilização de tecnologias de codificação padrão da indústria comercialmente disponíveis.

- Os dados pessoais apresentados por meio do Serviço minFraud possuem um comando (*token*) tal que os dados não poderão mais ser atribuídos a um indivíduo específico sem o uso de informações adicionais. Os dados que possuem esse token e as informações adicionais são armazenados separadamente e sujeitos a controles de acesso descritos acima.

13. Privacidade dos Dados e Medidas de Proteção

- A MaxMind implementou políticas e processos para garantir que os dados pessoais sejam processados adequadamente do início ao fim do ciclo de vida desses dados (desde a coleta e durante o uso, divulgação e destruição).

- A MaxMind implementou um processo de solicitações de dados do titular para garantir os direitos do titular dos dados de acordo com a legislação de proteção de dados aplicável. A MaxMind está comprometida com o respeito a esses direitos e a garantia de que a MaxMind responderá às solicitações dos titulares de dados de forma transparente, legal, correta e isenta.

- A MaxMind mantém um registro de todas as solicitações recebidas dos titulares dos dados e as medidas tomadas para atender a essas solicitações. A MaxMind fornecerá todo suporte adequado aos clientes na resposta às solicitações dos titulares dos dados, quando solicitada, e de acordo com os contratos com eles assinados.

- As processadoras da MaxMind devem assinar os contratos adequados que regem o processamento e a proteção de dados pessoais e exigir as mesmas obrigações, conforme delineadas no Adendo, a serem transferidos para quaisquer outras processadoras que a MaxMind venha a contratar. A MaxMind compromete-se a efetuar todos os esforços adequados para garantir que os Contratos de Processamento de Dados sejam assinados por suas processadoras.

- A MaxMind baseia-se nas Cláusulas Contratuais Padrão para apoiar a transferência legal de dados pessoais para fora do país onde foram originalmente coletados e possui contratos adequados assinados com suas subsidiárias, afiliadas, processadoras, subprocessadoras e clientes para comprovar as transferências entre fronteiras.

Anexo 4

Descrição do Processamento / Transferência

Módulo 1 (transferências de controladora para controladora)

A. LISTA DAS PARTES

Exportadora(s) de Dados:

1.	Nome:	MaxMind, Inc.
	Endereço:	14 Spring Street, #3, Waltham, Massachussetts 02451, Estados Unidos
	Nome, cargo e detalhes de contato da pessoa de contato:	MaxMind, Inc. Departamento Jurídico e-mail: legal@maxmind.com MaxMind DPO email: dpo@maxmind.com MaxMind, Inc. Diretor de Proteção de Dados 14 Spring Street, 3rd floor, Waltham, Massachussetts 02451, Estados Unidos Representante perante a Regulamentação (EU) 2016/679 GDPR Formulário de solicitação on-line: https://edpo.com/gdpr-data-request/ EDPO Block 1, Blanchardstown Corporate Park, Ballycoolin Rd, Dublin D15 AKK1, Irlanda Representante perante a Regulamentação (EU) 2016/679 GDPR Formulário de solicitação on-line: https://edpo.com/uk-gdpr-data-request/ EDPO UK 8 Northumberland Avenue, Londres WC2N 5BY, Reino Unido
	Atividades relevantes para os dados transferidos nos termos destas Cláusulas:	Fornecimento dos Serviços descritos no Contrato.
	Função:	Controladora

Importadora(s) de dados:

1.	Nome:	Parte identificada como “Você” no Adendo
	Endereço	O endereço para avisos fornecido por você à

		MaxMind
	Nome, cargo e detalhes de contato da pessoa de contato:	A pessoa de contato, cargo dessa pessoa e detalhes de contato fornecidos por você à MaxMind.
	Atividades relevantes para os dados transferidos nos termos destas Cláusulas:	Utilizando os Serviços descritos no Contrato para os fins descritos no Contrato.
	Função:	Controladora

B. DESCRIÇÃO DA TRANSFERÊNCIA

Categorias de titulares de dados cujos dados pessoais são transferidos:	Indivíduos associados aos Endereços de IP fornecidos pela MaxMind
Categorias de dados pessoais transferidos:	Endereços de IP e dados associados
Dados sensíveis transferidos (se aplicável) e restrições ou salvaguardas aplicadas que levam em consideração integralmente a natureza dos dados e os riscos envolvidos, tais como, por exemplo, rigorosa limitação de finalidade, restrições de acesso (incluindo-se acesso apenas para o quadro de pessoal que tenha efetuado treinamento especializado), mantendo um registro de acesso aos dados, restrições para transferências subsequentes ou medidas de segurança adicionais:	Quaisquer dados sensíveis não serão transferidos.
A frequência da transferência (por ex., se os dados são transferidos numa base pontual ou de maneira contínua):	Contínua – os dados serão transferidos periodicamente durante o prazo do Contrato.
Natureza do processamento:	Transmissão de dados para Você para suas finalidades conforme permitidas no Contrato.
Finalidade(s) da transferência de dados e processamentos adicionais:	Para as finalidades com base nos Serviços utilizados de acordo com o Contrato, incluindo-se o fornecimento de serviços de Geolocalização de IP, detecção de fraudes e serviços relacionados.
O período pelo qual os dados pessoais estarão retidos, ou, se isso não for possível, os critérios utilizados para estabelecer esse período:	Os dados poderão ser retidos pelos períodos especificados no Contrato.
Para transferências para (sub-) processadoras, especificar também o	Não disponível

assunto, a natureza e duração do processamento:	

C. AUTORIDADE SUPERVISORA COMPETENTE

Identificar a(s) autoridade(s) supervisora(s) competente(s) de acordo com a Cláusula 13 das SCCSs da UE (se aplicável)	Autoridade Supervisora Irlandesa

Anexo 5

Medidas de Segurança Organizacional e Técnica

Medida	Descrição
Medidas de pseudo-anonimização e criptografia de dados pessoais	Você garantirá que aprova as seguintes medidas de criptografia ao utilizar os Serviços da MaxMind: ● Criptografia HTTPS para dados em trânsito utilizando TLS 1.2 AES-256-GCM ou TLS 1.3 AES-128-GCM em toda interface de login e todo canal de comunicação da rede do sistema de informações. ● Criptografia Total do Disco dos dados em repouso utilizando o algoritmo AES-256-GCM padrão da indústria.
Medidas para garantir contínua confidencialidade, integridade, disponibilidade e flexibilidade dos sistemas e serviços de processamento	• Garantir que todos os usuários de contas tenham senhas seguras e fortes que sejam regularmente atualizadas. • Analisar regularmente usuários e permissões se você utiliza acesso de múltiplos usuários à conta. o Não compartilhe contas e senhas de usuário, e desative quaisquer contas de usuário se não são mais utilizadas. • Considere seu código de licença como uma senha, e armazene-o com segurança (por ex., num gestor de senhas) • Faça o login no local para que todos os sistemas de informações gravem informações suficientes para servir as necessidades operacionais, preservem a

	obrigação de prestar contas, e detectem atividade maliciosa. • Medidas flexíveis incluindo-se redundância construída dentro da sua infraestrutura e arquitetura de serviços, bem como proteção adequada dos seus backups. • Para automatização para baixar os GeoIP, utilize a versão de Atualização do GeoIP 3.1.1 ou mais recente.
Medidas para garantir a capacidade de recuperar a disponibilidade dos dados e o acesso a estes de maneira tempestiva no caso de um incidente físico ou técnico.	• Planejamento da Continuidade e Plano de Recuperação de Catástrofes • Procedimentos para enfrentar incidentes e reportá-los (gestão de incidentes) incluindo-se a detecção de possíveis incidentes de segurança e reação a eles.
Processos para testar, analisar e avaliar a efetividade de medidas técnicas e organizacionais a fim de garantir a segurança do processamento.	• Testagem regular de equipamentos de emergência, controles técnicos e processos.
Medidas para identificação e autorização de usuário	• Interconexões de rede seguras garantidas por VPN [*Rede Virtual Privada*], MFA [*autenticação multi-fatorial*], firewalls, etc. • Registro de transmissões de dados dos sistemas de informações que armazenam ou processam dados pessoais. • Autenticação de registros e acesso ao sistema monitorado. • O acesso aos dados necessários para a realização de um trabalho específico é garantido dentro dos sistemas de informações e aplicativos por uma função correspondente e conceito de autorização de acordo com o princípio de “necessitar saber”.

Medidas para a proteção de dados durante a transmissão	• Criptografia HTTPS para dados em trânsito utilizando TLS [*segurança das camadas de transporte*] v1.2+ ou mais recente. • Para automatização para fazer downloads do GeoIP, utilize a versão de Atualização do GeoIP 3.1.1 ou mais recente.
Medidas para a proteção de dados durante armazenagem	• Entradas no sistema registradas por meio de arquivos de registro • Listas de Controle de Acesso definindo os usuários que têm acesso e qual nível de acesso, de acordo com os princípios de "necessitar saber" e "privilégio mínimo".
Medidas para assegurar a segurança física dos locais nos quais os dados pessoais são processados	• Se um centro de dados for utilizado, assegurar que detém certificados válidos que garantem a segurança física, incluindo-se SOC 2, ISO/IEC, ou SAEE. • Se um centro de dados não for utilizado, garantir que o nível adequado de segurança física está instalado de acordo com as estruturas aceitáveis da indústria incluindo-se SOC ou ISO/IEC.
Medidas para garantir o registro [*logging*] de eventos	• Procedimentos instalados para examinar os registros regularmente. • Monitoramento instalado para eventos de falhas de registro. • Registro remoto • Replicação
Medidas para garantir a configuração do sistema, incluindo-se configuração padrão	• Política e Procedimentos de Controle de Acesso • Identificação da configuração do (baseline) parâmetro • Planejamento e Gestão da Configuração

	• Gestão da Alteração da Configuração • Contabilidade da Situação da Configuração • Verificação e Auditorias da Configuração • Gestão do dispositivo móvel
Medidas para governança e gestão da segurança da Tecnologia da Informação (TI) e TI interna	• Pessoa identificada e exclusiva para supervisionar a segurança das informações e o programa de compliance da organização. • Pessoal de segurança da rede e de informações.
Medidas para certificação/garantia dos processos e produtos	• Procedimentos instalados para segurança interna das informações ou auditorias de gestão da qualidade de acordo com as normas aprovadas da indústria tais como ISO/IEC, SOC, ou SSAE 16
Medidas para garantir a minimização de dados	• Restringir acesso a dados pessoais às partes envolvidas no processamento de acordo com princípio de "precisar saber" e de acordo com a função por trás da criação de perfis de acesso diferenciados. • Limites rigorosos do prazo para retenção de dados e mecanismos operacionais que garantem o cumprimento (por ex., deletar dados automaticamente após o prazo pré-definido). • Barreiras tecnológicas para fazer links não autorizados para fontes de dados independentes. • Limitação do nível de detalhes utilizado no processamento de dados pessoais: por exemplo, por meio de técnicas tais como privacidade diferenciada, anonimidade k, e medida adicional de obscurecimento e barulho.

	• Eliminação de metadados gerados durante determinados processos que não são necessários para o objetivo almejado.
Medidas para garantir a qualidade de dados	• Processo para o exercício de direitos de proteção de dados (direito de alterar e atualizar informações). • Estrutura de canal de dados para evitar dados duplicados. • Garantia do cumprimento da integridade dos dados
Medidas para garantir a retenção limitada de dados	• Controles automatizados para garantir a eficácia e confiabilidade dos cronogramas de retenção. • Testagem regular de controles automatizados para garantir a eficácia e confiabilidade dos cronogramas de retenção.
Medidas para garantir a obrigação de prestar contas	• Delegar responsabilidade para garantir a privacidade do usuário final do início ao fim do ciclo de vida do produto e por meio de processos comerciais aplicáveis. • Avaliações de impacto na proteção de dados como parte integrante de qualquer iniciativa de novo processamento. • Documentar todas as decisões que são adotadas dentro da organização de uma perspectiva de "privacidade com foco no projeto [*design thinking*]".
Medidas para permitir portabilidade de dados e garantir que sejam apagados	• Processos documentados em relação ao exercício pelos usuários de seus direitos de privacidade (por ex., direito de apagar ou direito de portabilidade dos dados). • Utilização de formatos abertos tais como CSV, XML ou JSON.