Termos de Processamento de Dados do Google Ads

O Google e a contraparte que concorda com estes termos ("**Cliente**") celebraram um contrato de prestação de Serviços de Operador (sujeito a alterações periódicas, o "**Contrato**").

Estes Termos de Processamento de Dados do Google Ads (incluindo os apêndices, "**Termos de Processamento de Dados**") são celebrados entre o Google e o Cliente e suplementam o Contrato. A partir do Início da Vigência dos Termos, estes Termos de Processamento de Dados entrarão em vigor e substituirão quaisquer termos anteriormente aplicáveis relativos ao objeto em questão, incluindo quaisquer adendos ou emendas sobre processamento de dados com relação aos Serviços de Operador.

Ao aceitar estes Termos de Processamento de Dados em nome do Cliente, você garante que: (a) tem autorização legal para submeter o Cliente aos Termos de Processamento de Dados; (b) leu e entendeu estes Termos de Processamento de Dados; e (c) em nome do Cliente, concorda com estes Termos de Processamento de Dados. Se você não tem autorização legal para aceitar em nome do Cliente, não aceite estes Termos de Processamento de Dados.

1. Introdução

Estes Termos de Processamento de Dados refletem o acordo das partes sobre os termos que regem o tratamento de determinados dados em relação à Legislação Europeia de Proteção de Dados e outras Legislações Não Europeias de Proteção de Dados.

2. Definições e interpretação

2.1 Nestes Termos de Processamento de Dados:

"**Produto Adicional**": um produto, serviço ou aplicativo fornecido pelo Google ou por um terceiro que: (a) não faz parte dos Serviços de Operador; e (b) está acessível para uso na interface do usuário dos Serviços de Operador ou, de alguma forma, integrado a eles.

"**Termos Adicionais para Legislações Não Europeias de Proteção de Dados**": os termos adicionais mencionados no Apêndice 3 refletem o acordo entre as partes sobre os termos que regem o tratamento de determinados dados em relação a certas Legislações Não Europeias de Proteção de Dados.

"**Afiliado**": qualquer entidade que, direta ou indiretamente, controle, seja controlada ou esteja sob o controle comum de uma das partes.

"**Dados Pessoais do Cliente**": dados pessoais que são tratados pelo Google em nome do Cliente ao fornecer os Serviços de Operador.

"**Incidente de Segurança**": uma violação da segurança do Google que gera destruição, perda, alteração, divulgação não autorizada de ou acesso acidentais ou ilegais a Dados Pessoais do Cliente em sistemas gerenciados ou controlados pelo Google. "Incidentes de Segurança" não incluem atividades ou tentativas malsucedidas que não comprometem a segurança dos Dados

Pessoais do Cliente, incluindo tentativas não concretizadas de login, pings, verificação de portas, ataques de negação de serviço e outros ataques de rede em firewalls ou sistemas de rede.

"**Ferramenta de Titulares de Dados**": uma ferramenta (se houver) disponibilizada por uma Entidade do Google aos titulares de dados pessoais que permite ao Google responder diretamente e de maneira padronizada a determinadas solicitações feitas por titulares com relação aos Dados Pessoais do Cliente. Por exemplo, configurações de publicidade on-line ou desativação do plug-in de um navegador.

"**EEE**": Espaço Econômico Europeu.

"**GDPR da União Europeia**": é o Regulamento (UE) 2016/679 do Parlamento e Conselho Europeu de 27 de abril de 2016 sobre a proteção de pessoas naturais em relação ao tratamento de dados pessoais, a livre transferência de tais dados e a revogação da Diretiva 95/46/EC.

"**Legislação Europeia de Proteção de Dados**": significa, conforme aplicável: (a) o GDPR; e/ou (b) a Lei Federal de Proteção de Dados de 19 de junho de 1992 (Suíça).

"**Leis Europeias ou Nacionais**": conforme aplicável, (a) a legislação da UE ou de estado-membro da UE (caso o GDPR da UE seja aplicável ao processamento de Dados Pessoais do Cliente); e/ou (b) a lei do Reino Unido ou de uma parte do Reino Unido (caso o GDPR Britânico seja aplicável ao processamento de Dados Pessoais do Cliente).

"**GDPR**": conforme aplicável: (a) o GDPR da União Europeia; e/ou (b) o GDPR do Reino Unido.

"**Google**": a Entidade do Google que é uma parte do Contrato.

"**Suboperadores da Afiliada do Google**": têm seu significado definido na Seção 11.1 (Consentimento para contratação de Suboperadores).

"**Entidade do Google**": Google LLC (anteriormente chamada de "Google Inc."), Google Ireland Limited ou qualquer outra Afiliada da Google LLC.

"**Certificação ISO 27001**": é a certificação ISO/IEC 27001:2013 ou qualquer certificação equivalente para os Serviços de Operador.

"**Cláusulas Contratuais Padrão**": as disposições em https://privacy.google.com/businesses/processorterms/mccs

"**Legislação Não Europeia de Proteção de Dados**" : leis de proteção de dados pessoais ou privacidade em vigor fora do EEE, da Suíça e do Reino Unido.

"**Endereço de E-mail para Notificação**": o endereço de e-mail (se houver) designado pelo Cliente, por meio da interface do usuário dos Serviços de Operador ou outros meios fornecidos pelo Google, para receber notificações relacionadas a estes Termos de Processamento de Dados.

"**Serviços de Operador**": os serviços aplicáveis listados em privacy.google.com/businesses/adsservices.

"**Documentação de Segurança**": o certificado emitido para a Certificação ISO 27001 e qualquer outra certificação ou documentação de segurança que o Google possa disponibilizar em relação aos Serviços de Operador.

"**Medidas de Segurança**": têm seu significado definido na Seção 7.1.1 (Medidas de Segurança do Google).

"**Suboperadores**": terceiros autorizados por meio destes Termos de Processamento de Dados a ter acesso e tratar Dados Pessoais do Cliente a fim de fornecer partes dos Serviços de Operador e qualquer suporte técnico relacionado.

"**Autoridade Supervisora**": conforme aplicável: (a) uma "autoridade supervisora" conforme definição no GDPR da União Europeia; e/ou (b) o "Comissário" conforme definição no GDPR do Reino Unido.

"**Período**": o tempo entre o Início da Vigência dos Termos e o final do fornecimento dos Serviços de Operador pelo Google de acordo com o Contrato.

"**Início da Vigência dos Termos**": significa, conforme aplicável:

(a) 25 de maio de 2018, se o Cliente clicou para aceitar ou se as partes concordaram com estes Termos de Processamento de Dados antes ou nesta data; ou

(b) a data em que o Cliente clicou para aceitar ou as partes concordaram com estes Termos de Processamento de Dados, se essa data for posterior a 25 de maio de 2018.

"**Suboperadores Terceirizados**": têm seu significado definido na Seção 11.1 (Consentimento para Contratação de Suboperadores).

"**GDPR do Reino Unido**": o GDPR da União Europeia conforme alterado e incorporado à legislação britânica, de acordo com os termos da UK European Union Withdrawal Act 2018 (Lei de Saída do Reino Unido da União Europeia de 2018), caso em vigor.

2.2 Os termos "**controlador**", "**titular de dados pessoais**", "**dados pessoais**", "**tratamento**" e "**operador**" quando usados nestes Termos de Processamento de Dados terão o significado atribuído a eles no GDPR, e os termos "**importador de dados**" e "**exportador de dados**" terão o significado atribuído a eles nas Cláusulas Contratuais Padrão.

2.3 As palavras "**incluir**" e "**incluindo**" significam "incluindo, entre outros". Todos os exemplos nestes Termos de Processamento de Dados são ilustrativos, e não constituem exemplos únicos de um conceito específico.

2.4 Qualquer referência a um enquadramento legal, estatuto ou outro ato legislativo é uma referência a ele conforme alterado ou promulgado de forma periódica.

2.5 Se os Termos de Processamento de Dados forem traduzidos para outros idiomas e houver inconsistência entre o texto em inglês e o texto traduzido, o texto em inglês prevalecerá.

3. Duração destes Termos de Processamento de Dados

Estes Termos de Processamento de Dados entrarão em vigor no Início da Vigência dos Termos e, não obstante a expiração do Período, permanecerão em vigor até a exclusão de todos os Dados Pessoais do Cliente pelo Google e expirarão automaticamente após esse fato, conforme descrito nestes Termos de Processamento de Dados.

4. Aplicação destes Termos de Processamento de Dados

4.1 **Aplicação da Legislação Europeia de Proteção de Dados**. As seções de 5 (Tratamento de Dados) a 12 (Contato com o Google; Registros de tratamento) serão empregadas somente na

medida em que a Legislação Europeia de Proteção de Dados for aplicável ao tratamento dos Dados Pessoais do Cliente, inclusive:

(a) o tratamento é entendido no contexto das atividades de um estabelecimento de Cliente no EEE ou no Reino Unido; e/ou

(b) Dados Pessoais do Cliente são dados pessoais relacionados a titulares de dados pessoais no EEE ou no Reino Unido e o tratamento se refere à oferta de bens ou serviços a esses titulares de dados pessoais ou ao monitoramento do comportamento deles no EEE ou no Reino Unido.

4.2 **Aplicação aos Serviços de Operador**. Estes Termos de Processamento de Dados serão aplicados apenas aos Serviços de Operador para os quais as partes tenham concordado com sua aplicação, por exemplo, (a) os Serviços de Operador para os quais o Cliente tenha aceitado estes Termos de Processamento de Dados ou (b) se o Contrato incorpora estes Termos de Processamento de Dados por referência, os Serviços de Operador que são objeto deste Contrato.

4.3 **Incorporação dos Termos Adicionais da Legislação Não Europeia de Proteção de Dados**. Os Termos Adicionais para Legislação Não Europeia de Proteção de Dados complementam estes Termos de Processamento de Dados.

5. Tratamento de Dados

5.1 **Funções e Conformidade com leis locais; Autorização**.

5.1.1 **Responsabilidades do Operador e do Controlador**. As partes confirmam e concordam que:

(a) o Apêndice 1 descreve o objeto em questão e os detalhes do tratamento de Dados Pessoais do Cliente;

(b) o Google é um operador de Dados Pessoais do Cliente de acordo com a Legislação Europeia de Proteção de Dados;

(c) o Cliente é um controlador ou operador, conforme aplicável, de Dados Pessoais do Cliente, de acordo com a Legislação Europeia de Proteção de Dados; e

(d) cada parte cumprirá as obrigações aplicáveis de acordo com a Legislação Europeia de Proteção de Dados em relação ao tratamento de Dados Pessoais do Cliente.

5.1.2 **Autorização por um Controlador Terceiro**. Se o Cliente for um operador, ele garantirá ao Google que as instruções e ações em relação a Dados Pessoais do Cliente foram emitidas e autorizadas pelo controlador em questão, incluindo a indicação do Google como outro operador.

5.2 **Instruções do Cliente**. Ao celebrar estes Termos de Tratamento de Dados, o Cliente instrui o Google a tratar os Dados Pessoais do Cliente somente de acordo com a legislação aplicável: (a) a fim de prestar os Serviços de Operador e qualquer outro suporte técnico relacionado; (b) conforme o uso dos Serviços de Operador por parte do Cliente (incluindo nas configurações e em outras funcionalidades dos Serviços de Operador) e com qualquer outro suporte técnico relacionado; (c) conforme documentado no formulário do Contrato, incluindo estes Termos de Processamento de Dados; e (d) conforme documentado em quaisquer outras instruções por escrito fornecidas pelo Cliente e reconhecidas pelo Google como Instruções do Cliente para fins destes Termos de Processamento de Dados.

5.3 **Conformidade do Google com as Instruções**. O Google obedecerá às instruções descritas na Seção 5.2 (Instruções do Cliente), incluindo aquelas relativas à transferência de dados, a menos que Leis Europeias ou Nacionais a que o Google está sujeito exijam outro tratamento de Dados Pessoais do Cliente pelo Google. Nesse caso, o Google informará ao Cliente, exceto se alguma dessas leis proibir tal aviso por motivos de interesse público.

5.4 **Produtos Adicionais**. Se o Cliente usar qualquer Produto Adicional, os Serviços de Operador poderão permitir que tal produto acesse Dados Pessoais do Cliente quando necessário para a interoperação do Produto Adicional com os Serviços de Operador. Para fins de esclarecimento, estes Termos de Processamento de Dados não se aplicam ao tratamento de dados pessoais relacionado ao fornecimento de qualquer Produto Adicional usado pelo Cliente, incluindo dados pessoais transmitidos para tal Produto Adicional ou por meio dele.

6. Exclusão de Dados

6.1 **Exclusão durante o Período**.

6.1.1 **Serviços de Operador com Funcionalidade de Exclusão**. Durante o Período, se:

(a) a funcionalidade dos Serviços de Operador incluir a opção para que o Cliente exclua os Dados Pessoais do Cliente;

(b) o Cliente usar os Serviços de Operador para excluir determinados Dados Pessoais do Cliente; e

(c) os Dados Pessoais do Cliente excluídos não puderem ser recuperados pelo Cliente (por exemplo, da "Lixeira"),

o Google excluirá tais Dados Pessoais do Cliente dos sistemas assim que razoavelmente possível e dentro de um período máximo de 180 dias, exceto se as Leis Europeias ou Nacionais exigirem a retenção.

6.1.2 **Serviços de Operador sem Funcionalidade de Exclusão**. Durante o Período, se a funcionalidade dos Serviços de Operador não incluir a opção para que o Cliente exclua os Dados Pessoais do Cliente, o Google cumprirá:

(a) a qualquer solicitação razoável do Cliente para facilitar tal exclusão, na medida em que isso seja possível dada a natureza e a funcionalidade dos Serviços de Operador e exceto se as Leis Europeias ou Nacionais exigirem a retenção; e

(b) às práticas de retenção de dados descritas em https://policies.google.com/technologies/ads.

O Google poderá cobrar uma taxa, com base em custos razoáveis, por qualquer exclusão de dados de acordo com a Seção 6.1.2(a). O Google dará ao Cliente mais detalhes sobre as taxas aplicáveis e sobre a base de cálculo delas antes de qualquer exclusão.

6.2 **Exclusão ao Término do Período**. Ao Término do Período, o Cliente instruirá o Google a excluir todos os Dados Pessoais do Cliente (incluindo cópias) dos sistemas do Google, de acordo com a legislação aplicável. O Google cumprirá essa instrução assim que razoavelmente possível e dentro de um período máximo de 180 dias, exceto se as Leis Europeias ou Nacionais exigirem a retenção.

7. Segurança das Informações

7.1 **Medidas e Assistência de Segurança do Google.**

7.1.1 **Medidas de Segurança do Google**. O Google implementará e manterá medidas técnicas e organizacionais para proteger os Dados Pessoais do Cliente contra destruição, perda, alteração, divulgação não autorizada ou acesso acidentais ou ilegais, conforme descrito no Apêndice 2 (as "**Medidas de Segurança**"). De acordo com esse apêndice, as Medidas de Segurança incluem ações para: (a) criptografar dados pessoais; (b) ajudar a garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas de sistemas e serviços do Google; (c) ajudar a restaurar o acesso a dados pessoais em tempo hábil após um incidente; e (d) fazer testes de eficiência regulares. O Google pode atualizar ou modificar as Medidas de Segurança periodicamente, desde que tais atualizações e modificações não resultem na diminuição do nível de segurança geral dos Serviços de Operador.

7.1.2 **Conformidade de Segurança pela Equipe do Google**. O Google tomará as providências cabíveis para garantir conformidade com as Medidas de Segurança por parte dos funcionários, prestadores de serviços e Suboperadores de acordo com o escopo aplicável, incluindo a garantia de que todas as pessoas autorizadas a tratar Dados Pessoais do Cliente assumam as obrigações adequadas de confidencialidade.

7.1.3 **Assistência de Segurança do Google**. O Cliente concorda que o Google, considerando a natureza do tratamento de Dados Pessoais do Cliente e as informações disponíveis, ajudará o Cliente a garantir a conformidade com todas as obrigações do Cliente relacionadas à segurança de dados pessoais, incluindo, se aplicável, as obrigações do Cliente relativas aos Artigos 32 a 34, inclusive, do GDPR, por meio de:

(a) implementação e manutenção das Medidas de Segurança de acordo com a Seção 7.1.1 (Medidas de Segurança do Google);

(b) cumprimento dos termos da Seção 7.2 (Incidentes de Segurança); e

(c) fornecimento ao Cliente da Documentação de Segurança de acordo com a Seção 7.5.1 (Análises de Documentação de Segurança) e das informações contidas nestes Termos de Processamento de Dados.

7.2 **Incidentes de Segurança**.

7.2.1 **Notificação de Incidentes**. Se o Google tomar conhecimento de um Incidente de Segurança, ele: (a) notificará o Cliente imediatamente e sem qualquer atraso; e (b) tomará providências razoáveis imediatas para minimizar os danos e proteger os Dados Pessoais do Cliente.

7.2.2 **Detalhes do Incidente de Segurança**. Notificações feitas conforme previsto na Seção 7.2.1 (Notificação de Incidentes) descreverão, na medida do possível, detalhes do Incidente de Segurança, incluindo as ações realizadas para reduzir os possíveis riscos e as etapas que o Google recomenda que o Cliente siga para resolver o problema.

7.2.3 **Envio da Notificação**. O Google enviará a notificação sobre um Incidente de Segurança ao Endereço de E-mail para Notificação ou, a critério do Google (inclusive se o Cliente não tiver fornecido esse endereço), por comunicação direta (por exemplo, por telefone ou pessoalmente). O Cliente é a única parte responsável por fornecer o Endereço de E-mail para Notificação e garantir que esse endereço esteja atualizado e seja válido.

7.2.4 **Notificações a Terceiros**. O Cliente é a única parte responsável por obedecer às leis de notificação de incidentes aplicáveis ao Cliente e cumprir todas as obrigações de notificação a

terceiros relacionadas a Incidentes de Segurança.

7.2.5 **Não Reconhecimento de Falha por parte do Google**. A notificação ou resposta do Google a um Incidente de Segurança nos termos desta Seção 7.2 (Incidentes de Segurança) não será interpretada como um reconhecimento por parte do Google de qualquer falha ou responsabilidade em relação ao Incidente de Segurança.

7.3 **Responsabilidades e Avaliação de Segurança do Cliente**.

7.3.1 **Responsabilidades de Segurança do Cliente**. O Cliente concorda que, sem prejuízos às obrigações do Google conforme previsto nas Seções 7.1 (Medidas e Assistência de Segurança do Google) e 7.2 (Incidentes de Segurança):

(a) o Cliente é responsável pelo uso que fizer dos Serviços de Operador, incluindo:

(i) uso apropriado dos Serviços de Operador a fim de garantir um nível de segurança adequado considerando o risco aos Dados Pessoais do Cliente; e

(ii) proteção das credenciais de autenticação de contas, sistemas e dispositivos que o Cliente usa para ter acesso aos Serviços de Operador; e

(b) o Google não tem a obrigação de proteger Dados Pessoais do Cliente armazenados ou transferidos fora dos sistemas do Google ou dos Suboperadores dele.

7.3.2 **Avaliação de Segurança do Cliente**. O Cliente reconhece e concorda que (considerando a tecnologia avançada; os custos de implementação e a natureza; o escopo; o contexto e as finalidades do tratamento dos Dados Pessoais do Cliente; bem como os riscos para os indivíduos) as Medidas de Segurança implementadas e mantidas pelo Google definidas na Seção 7.1.1 (Medidas de Segurança do Google) fornecem um nível de segurança adequado considerando o risco aos Dados Pessoais do Cliente.

7.4 **Certificação de Segurança**. Para avaliar e ajudar a garantir a eficiência contínua das Medidas de Segurança, o Google manterá a Certificação ISO 27001.

7.5 **Análises e Auditorias de Conformidade**.

7.5.1 **Análises da Documentação de Segurança**. Para demonstrar a conformidade do Google com as suas obrigações de acordo com estes Termos de Processamento de Dados, o Google disponibilizará a Documentação de Segurança para análise do Cliente.

7.5.2 **Direitos de Auditoria do Cliente**.

(a) O Google permitirá que o Cliente ou um auditor terceirizado indicado pelo Cliente realize auditorias (incluindo inspeções) para verificar a conformidade do Google com as suas obrigações segundo estes Termos de Processamento de Dados, conforme previsto na Seção 7.5.3 (Termos Comerciais Adicionais para Auditorias). O Google contribuirá com tais auditorias, conforme descrito na Seção 7.4 (Certificação de Segurança) e nesta Seção 7.5 (Análises e Auditorias de Conformidade).

(b) Caso as Cláusulas Contratuais Padrão sejam aplicáveis de acordo com a Seção 10.2 (Transferência de Dados), o Google autorizará o Cliente ou um auditor terceirizado indicado pelo Cliente a conduzir auditorias conforme descrito nas Cláusulas Contratuais Padrão de acordo com a seção 7.5.3 (Termos Comerciais Adicionais para Auditorias).

(c) O Cliente também pode realizar uma auditoria para verificar a conformidade do Google com suas obrigações segundo estes Termos de Processamento de Dados analisando o certificado emitido para a Certificação ISO 27001, que reflete o resultado de uma auditoria realizada por um auditor terceiro.

7.5.3 **Termos Comerciais Adicionais para Auditorias**.

(a) O Cliente enviará ao Google qualquer solicitação para uma auditoria de acordo com a Seção 7.5.2(a) ou 7.5.2(b), conforme previsto na Seção 12.1 (Contato com o Google).

(b) Depois de receber uma solicitação de acordo com a Seção 7.5.3(a), o Google discutirá com o Cliente e chegará a um acordo prévio sobre a data de início, o escopo e a duração razoáveis de qualquer auditoria prevista na Seção 7.5.2(a) ou 7.5.2(b), além de controles de confidencialidade e segurança aplicáveis.

(c) O Google poderá cobrar uma taxa, com base nos custos razoáveis, para qualquer auditoria prevista na Seção 7.5.2(a) ou 7.5.2(b). O Google fornecerá ao Cliente mais detalhes sobre qualquer taxa aplicável e sobre a base de cálculo. O Cliente será responsável pelas taxas cobradas por um auditor terceirizado indicado por ele para executar a auditoria.

(d) O Google poderá se opor a qualquer auditor terceirizado indicado pelo Cliente para realizar auditorias previstas na Seção 7.5.2(a) ou 7.5.2(b) se, segundo opinião razoável do Google, o auditor não estiver devidamente qualificado, não for um auditor independente, for um concorrente do Google ou for claramente inadequado. Qualquer objeção feita pelo Google exigirá que o Cliente indique outro auditor ou conduza a auditoria por conta própria.

(e) Nada nestes Termos de Processamento de Dados exige que o Google permita o acesso ou divulgue, seja ao Cliente, seja ao auditor terceiro:

(i) dados de outro cliente de uma Entidade do Google;

(ii) informações financeiras ou contábeis internas de uma Entidade do Google;

(iii) segredos comerciais de uma Entidade do Google;

(iv) informações que, na opinião razoável do Google, possam: (A) comprometer a segurança dos sistemas ou instalações de qualquer Entidade do Google; ou (B) fazer com que uma Entidade do Google deixe de cumprir as obrigações previstas na Legislação Europeia de Proteção de Dados ou as obrigações de segurança e/ou privacidade para com o Cliente ou com terceiros; ou

(v) informações que o Cliente ou o auditor terceirizado tentem acessar por qualquer motivo que não seja o cumprimento de boa-fé das obrigações do Cliente segundo a Legislação Europeia de Proteção de Dados.

7.5.4 **Não Modificação das Cláusulas Contratuais Padrão**. Caso o as Cláusulas Contratuais Padrão sejam aplicáveis de acordo com a Seção 10.2 (Transferência de Dados), nada nesta Seção 7.5 (Análises e Auditorias de Conformidade) altera ou modifica quaisquer direitos ou obrigações do Cliente ou do Google LLC conforme as Cláusulas Contratuais Padrão.

8. Avaliações de Impacto e Consultas

O Cliente concorda que o Google, considerando a natureza do tratamento e das informações disponibilizadas, auxilie o Cliente a garantir a conformidade com todas as obrigações relativas a avaliações de impacto de proteção de dados e consultoria prévia, incluindo, se aplicável, as obrigações do Cliente previstas nos Artigos 35 e 36 do GDPR, por meio das seguintes ações:

(a) fornecimento da Documentação de Segurança prevista na Seção 7.5.1 (Análises de Documentação de Segurança);

(b) fornecimento das informações contidas nestes Termos de Processamento de Dados; e

(c) fornecimento ou disponibilização, de acordo com práticas padrão do Google, de outros materiais referentes à natureza dos Serviços de Operador e ao tratamento de Dados Pessoais do Cliente (por exemplo, materiais da Central de Ajuda).

9. Direitos do Titular de Dados

9.1 **Respostas a Solicitações de Titulares de Dados**. Se o Google receber uma solicitação de um titular de dados pessoais relativa a Dados Pessoais do Cliente, ele:

(a) responderá diretamente à solicitação do titular de dados pessoais, de acordo com a funcionalidade padrão da Ferramenta de Titulares de Dados, se a solicitação tiver sido feita por meio de tal ferramenta; ou

(b) aconselhará o titular de dados pessoais a enviar a solicitação ao Cliente para que ele a responda, se ela não tiver sido feita por meio da Ferramenta de Titulares de Dados.

9.2 **Assistência a Solicitações de Titulares de Dados do Google**. O Cliente concorda que o Google (considerando a natureza do tratamento de Dados Pessoais do Cliente e, se aplicável, o Artigo 11 do GDPR) ajude o Cliente a cumprir qualquer obrigação de responder a solicitações feitas por titulares de dados. Isso inclui, se aplicável, a obrigação de responder a solicitações para exercer os direitos de titular de dados previstos no Capítulo III do GDPR por meio das seguintes ações:

(a) fornecimento da funcionalidade dos Serviços de Operador;

(b) cumprimento do estipulado na Seção 9.1 (Respostas a Solicitações de Titulares de Dados); e

(c) disponibilização das Ferramentas de Titulares de Dados, se aplicável aos Serviços de Operador.

10. Transferência de Dados

10.1 **Instalações de Armazenamento e Tratamento de Dados**. O Cliente concorda que o Google pode, de acordo com o previsto na Seção 10.2 (Transferência de Dados), armazenar e tratar Dados Pessoais do Cliente em qualquer país em que o Google ou qualquer um dos Suboperadores dele mantenha instalações.

10.2 **Transferência de Dados**.

Caso o armazenamento e/ou processamento de Dados Pessoais do Cliente envolva transferência de tais dados do EEE, da Suíça ou do Reino Unido para qualquer país terceiro que não está sujeito a uma decisão de adequação conforme a Legislação Europeia de Proteção de Dados:

(a) o Cliente (como exportador de dados) considerado como tendo assinado as Cláusulas Contratuais Padrão com o Google LLC (como importador de dados);

(b) as transferências estarão sujeitas às disposições das Cláusulas Contratuais Padrão;

(c) o Google garantirá que o Google LLC cumpra com suas obrigações de acordo com as Cláusulas Contratuais Padrão a respeito de tais transferências.

10.3 **Informações de Data Center**. Informações sobre os data centers do Google estão disponíveis em www.google.com/about/datacenters/locations/.

11. Suboperadores

11.1 **Consentimento para a Contratação de Suboperadores**. O Cliente autoriza especificamente a contratação de Afiliados do Google como Suboperadores ("**Suboperadores Afiliados do Google**"). Além disso, o Cliente autoriza, de forma geral, a contratação de outros terceiros como Suboperadores ("**Suboperadores Terceirizados**"). Caso as Cláusulas Contratuais Padrão sejam aplicáveis de acordo com a Seção 10.2 (Transferência de Dados), as autorizações acima constituem o consentimento prévio por escrito do Cliente para a subcontratação pelo Google LLC do processamento dos Dados Pessoais do Cliente.

11.2 **Informações sobre Suboperadores**. Veja informações sobre os Suboperadores em privacy.google.com/businesses/subprocessors.

11.3 **Requisitos para a Contratação de Suboperadores**. Ao contratar qualquer Suboperador, o Google:

(a) garantirá, por meio de um contrato por escrito, que:

(i) o Suboperador só acesse e use os Dados Pessoais do Cliente conforme o necessário para cumprir as obrigações subcontratadas e o faça de acordo com o Contrato, incluindo estes Termos de Processamento de Dados, e, caso seja aplicável de acordo com a Seção 10.2 (Transferência de Dados), as Cláusulas Contratuais Padrão; e

(ii) as obrigações de proteção de dados definidas no Artigo 28(3) do GDPR sejam impostas ao Suboperador, caso o GDPR se aplique ao tratamento de Dados Pessoais do Cliente; e

(b) permanecerá totalmente responsável por todas as obrigações estipuladas e por todos os atos e omissões por parte do Suboperador.

11.4 **Oportunidade para Objeção quanto a Alterações de Suboperador**.

(a) Quando um novo Suboperador Terceirizado for contratado ao longo do Período, o Google, pelo menos 30 dias antes de o novo Suboperador Terceirizado tratar qualquer Dado Pessoal do Cliente, informará o Cliente sobre a contratação, incluindo o nome e a localização do Suboperador em questão e as atividades que ele executará. Isso será feito pelo envio de uma mensagem ao Endereço de E-mail para Notificação.

(b) O Cliente poderá se opor a qualquer novo Suboperador Terceirizado rescindindo o Contrato imediatamente mediante notificação por escrito ao Google, sob a condição de fornecer essa notificação em um prazo de 90 dias após ter sido informado sobre a contratação do novo Suboperador Terceirizado, conforme descrito na Seção 11.4(a). O direito de rescisão é medida exclusiva do Cliente em caso de objeção a qualquer novo Suboperador Terceirizado.

12. Contato com o Google; Registros de Tratamento

12.1 **Contato com o Google**. O Cliente pode entrar em contato com o Google em relação ao exercício dos direitos previstos nestes Termos de Processamento de Dados pelos métodos descritos em privacy.google.com/businesses/processorsupport ou por outros meios que possam ser fornecidos pelo Google oportunamente.

12.2 **Registros de Tratamento do Google**. O Cliente reconhece que o Google, de acordo com o GDPR, é obrigado a: (a) coletar e manter registros de informações específicas, incluindo o nome e detalhes de contato de cada operador e/ou controlador em nome do qual o Google está agindo e (se aplicável) do representante local e do encarregado de proteção de dados desse operador ou controlador; e (b) disponibilizar tais informações a qualquer Autoridade Supervisora. Da mesma forma, o Cliente, quando solicitado e se aplicável, fornecerá tais informações ao Google por meio da interface do usuário dos Serviços de Operador ou por outros meios que possam ser disponibilizados pelo Google e usará essa interface ou outros meios para garantir que todas as informações fornecidas sejam mantidas corretas e atualizadas.

13. Responsabilidade

13.1 Limite de Responsabilidade. Se o Contrato for regido pela legislação de:

(a) um estado dos Estados Unidos da América, apesar de qualquer disposição no Contrato, a responsabilidade total de qualquer uma das partes em relação à outra parte decorrente destes Termos de Processamento de Dados será limitada ao valor monetário máximo de acordo com a restrição de responsabilidade do Contrato. Para fins de esclarecimento, nenhuma exclusão por limitação de responsabilidade do Contrato será aplicada a reivindicações de indenização baseadas no Contrato quando relativas à Legislação Europeia de Proteção de Dados ou à Legislação Não Europeia de Proteção de Dados; ou

(b) uma jurisdição que não seja um estado dos Estados Unidos da América. Nesse caso, a responsabilidade das partes decorrente destes Termos de Processamento de Dados estará sujeita às exclusões e limitações de responsabilidade do Contrato.

13.2 Responsabilidade caso as Cláusulas Contratuais Padrão sejam Aplicáveis. Caso as Cláusulas Contratuais Padrão sejam aplicáveis conforme Seção 10.2 (Transferência de Dados), o valor total de responsabilidade do:

(a) Google LLC e Google para com o Cliente; e

(b) Cliente para com o Google LLC e Google,

conforme ou em conexão com o Contrato e as Cláusulas Contratuais Padrão combinados estarão sujeitos à Seção 13.1 (Limite de Responsabilidade).

14. Terceiros Beneficiários

Quando o Google LLC não for parte do Contrato e as Cláusulas Contratuais Padrão não aplicáveis conforme Seção 10.2 (Transferência de Dados), o Google LLC será um terceiro beneficiário das Seções 6.2 (Exclusão ao Término do Período), 7.5 (Análises e Auditorias de Conformidade), 9.1 (Respostas a Solicitações de Titulares de Dados), 10.2 (Transferência de Dados), 11.1

(Consentimento para a Contratação de Suboperadores) e 13.2 (Responsabilidade caso as Cláusulas Contratuais Padrão sejas Aplicáveis). À medida em que esta Seção 14 (Terceiros Beneficiários) entre em conflito ou seja inconsistente com qualquer cláusula no Contrato, esta Seção 14 (Terceiros Beneficiários) será aplicada.

15. Vigência destes Termos de Processamento de Dados

Em caso de qualquer conflito ou inconsistência entre as Cláusulas Contratuais Padrão, os Termos Adicionais da Legislação Não Europeia de Proteção de Dados, e o restante destes Termos de Processamento de Dados e/ou o restante do Contrato, será aplicada a seguinte ordem de precedência:

(a) as Cláusulas Contratuais Padrão;

(b) os Termos Adicionais para Legislação Não Europeia de Proteção de Dados;

(c) o restante destes Termos de Processamento de Dados; e

(d) o restante do Contrato.

Sujeito às alterações nestes Termos de Processamento de Dados, o Contrato permanece vigente.

16. Alterações nestes Termos de Processamento de Dados

16.1 **Alterações de URLs**. Periodicamente, o Google pode alterar qualquer URL mencionado nestes Termos de Processamento de Dados e o conteúdo de qualquer URL, com exceção de:

(a) o Google somente poderá mudar as Cláusulas Contratuais Padrão de acordo com as Seções 16.2(b) - 16.2(d) (Alterações aos Termos de Processamento de Dados) ou para incorporar qualquer nova versão das Cláusulas Contratuais Padrão que possa ser adotada conforme a Legislação Europeia de Proteção de Dados, em cada caso de modo que não afete a validade das Cláusulas Contratuais Padrão conforme a Legislação Europeia de Proteção de Dados; e

(b) O Google apenas alterará a lista de possíveis Serviços de Operador disponível em privacy.google.com/businesses/adsservices. para: (a) refletir uma mudança no nome de um serviço; (b) adicionar um novo serviço; ou (c) remover um serviço em que: (x) todos os contratos para a prestação de tal serviço estão rescindidos ou (y) o Google tenha o consentimento do Cliente.

16.2 **Alterações nos Termos de Processamento de Dados**. O Google poderá modificar estes Termos de Processamento de Dados se a alteração:

(a) for expressamente permitida por estes Termos de Processamento de Dados, inclusive conforme descrito na Seção 16.1 (Alterações de URLs);

(b) refletir uma alteração no nome ou na forma de uma entidade legal;

(c) for necessária para obedecer a uma lei ou regulamentação aplicável, ordens judiciais ou orientação expedida por um regulador ou agência governamental; ou

(d) não: (i) resultar em diminuição no nível da segurança geral dos Serviços de Operador; (ii) ampliar o escopo nem remover qualquer restrição, (x) no caso dos Termos Adicionais para

Legislação Não Europeia de Proteção de Dados, os direitos do Google de tratar os dados no escopo dos Termos Adicionais para Legislação Não Europeia de Proteção de Dados ou (y) no caso do restante destes Termos de Processamento de Dados, o processamento de Dados Pessoais do Cliente pelo Google, conforme descrito na Seção 5.3 (Conformidade do Google com as instruções); e (iii) resultar em impacto negativo significativo sobre os direitos do Cliente de acordo com estes Termos de Processamento de Dados, conforme razoavelmente determinado pelo Google.

16.3 **Notificação de Alterações**. Caso o Google tenha intenção de alterar estes Termos de Processamento de Dados conforme a Seção 16.2(c) ou (d), ele informará o Cliente no mínimo 30 dias antes de a alteração entrar em vigor, ou em um período menor, se exigido por lei ou regulamentação aplicável, por ordens judiciais ou orientação expedida por um regulador ou agência governamental. A alteração será feita (a) enviando uma mensagem ao Endereço de E-mail para Notificação ou (b) alertando o Cliente por meio da interface do usuário dos Serviços de Operador. Caso o Cliente se oponha a qualquer uma dessas alterações, ele poderá rescindir o Contrato enviando uma notificação por escrito ao Google em no máximo 90 dias após ter sido informado de tal alteração.

Apêndice 1: Objeto em Questão e Detalhes do Processamento de Dados

Objeto em questão

Prestação dos Serviços de Operador e de qualquer suporte técnico relacionado pelo Google ao Cliente.

Duração do tratamento

O Período, incluindo o tempo entre a expiração do Período e a exclusão de todos os Dados Pessoais do Cliente pelo Google de acordo com estes Termos de Processamento de Dados.

Natureza e finalidade do tratamento

O Google tratará os Dados Pessoais do Cliente com a finalidade de prestar os Serviços de Operador e qualquer suporte técnico relacionado ao Cliente de acordo com estes Termos de Processamento de Dados. O tratamento inclui coleta, registro, organização, estruturação, armazenamento, alteração, recuperação, uso, divulgação, combinação, exclusão e destruição, conforme aplicável aos Serviços de Operador e às instruções descritas na Seção 5.2 (Instruções do Cliente).

Tipos de dados pessoais

Os Dados Pessoais do Cliente podem incluir os tipos de dados pessoais descritos em privacy.google.com/businesses/adsservices.

Categorias de titulares de dados

Os Dados Pessoais do Cliente poderão ser enquadrados nestes tipos de categorias de titulares de dados:

- titulares de dados dos quais o Google coleta dados pessoais ao prestar os Serviços de Operador; e/ou
- titulares de dados cujos dados pessoais são transferidos para o Google em relação aos Serviços de Operador pelo Cliente, por instrução dele ou em nome dele.

Dependendo da natureza dos Serviços de Operador, esses titulares de dados podem incluir indivíduos: (a) a quem uma divulgação on-line tenha sido ou será direcionada; (b) que tenham visitado websites ou aplicativos específicos para os quais o Google presta os Serviços de Operador; e/ou (c) que sejam clientes ou usuários de produtos ou serviços do Cliente.

Apêndice 2: Medidas de Segurança

A partir do Início da Vigência dos Termos, o Google implementará e manterá as Medidas de Segurança definidas neste Apêndice 2. O Google pode atualizar ou modificar tais Medidas de Segurança periodicamente, desde que essas atualizações e modificações não resultem na diminuição do nível da segurança geral dos Serviços de Operador.

1. Data Center e Segurança de Rede

(a) **Data centers**

Infraestrutura. O Google mantém data centers distribuídos geograficamente. Ele armazena todos os dados em data centers fisicamente protegidos.

Contingência. Sistemas de infraestrutura foram criados para eliminar pontos únicos de falha e minimizar o impacto de riscos ambientais previstos. Circuitos duplos, interruptores, redes ou outros dispositivos necessários ajudam a proporcionar essa contingência. Os Serviços de Operador foram criados para permitir que o Google execute certos tipos de manutenção preventiva e corretiva sem interrupções. Todos os equipamentos e instalações documentaram procedimentos de manutenção preventiva que detalham o processo e a frequência de desempenho de acordo com as especificações internas ou do fabricante. A manutenção preventiva ou corretiva dos equipamentos dos data centers é agendada por meio de um processo padrão, de acordo com procedimentos documentados.

Energia. Os sistemas de energia elétrica dos data centers são desenvolvidos para serem contingentes e poderem passar por manutenção sem afetar as operações contínuas, 24 horas por dia, 7 dias por semana. Na maioria dos casos, é fornecida uma fonte de energia principal e uma alternativa, cada uma delas com a mesma capacidade, para componentes essenciais da infraestrutura do data center. Uma alimentação de reserva é fornecida por vários mecanismos, por exemplo, baterias de fonte de alimentação ininterrupta (UPS, na sigla em inglês), que oferecem proteção elétrica consistentemente confiável durante blecautes parciais da concessionária de serviços públicos, blecautes totais, sobretensão/subtensão e condições de frequência fora da tolerância. Se a energia for interrompida, a alimentação de reserva fornecerá eletricidade ao data center na capacidade total por até 10 minutos, até que os sistemas de geradores a diesel sejam acionados. Os geradores a diesel podem ser inicializados de forma automática em segundos para fornecer energia elétrica de emergência suficiente para alimentar o data center na capacidade total normalmente por um período de dias.

Sistemas operacionais de servidores. Os servidores do Google usam sistemas operacionais protegidos e personalizados para as necessidades exclusivas dos servidores da empresa. Os dados são armazenados usando algoritmos proprietários para aumentar a segurança e contingência desses dados. O Google emprega um processo de análise para aumentar a segurança do código usado para prestar os Serviços de Operador e aprimorar os produtos de segurança em ambientes de produção.

Continuidade dos negócios. O Google replica dados em vários sistemas para ajudar a proteger contra destruição ou perda acidental. O Google desenvolveu planejamento e testes regulares para recuperação de desastres/planejamento de continuidade dos negócios.

(b) **Redes e transmissão**.

Transmissão de dados. Os data centers geralmente são conectados por links privados de alta velocidade que proporcionam uma transferência de dados segura e rápida. Além disso, o Google criptografa os dados transmitidos entre data centers para evitar que os dados sejam lidos, copiados, alterados ou removidos sem autorização durante o transporte eletrônico. O Google transfere dados por meio de protocolos padrão da Internet.

Superfície de ataque externo. O Google emprega várias camadas de dispositivos de rede e detecção de invasões para proteger sua superfície de ataque externo. Ele considera os possíveis vetores de ataques e incorpora tecnologias específicas adequadas a sistemas externos.

Detecção de intrusões. A detecção de intrusões fornece informações sobre atividades de ataque em andamento e informações adequadas para responder a incidentes. A detecção de invasão do Google envolve:

1. controlar rigidamente o tamanho e a composição da superfície de ataque do Google por meio de medidas preventivas;
2. empregar controles inteligentes de detecção nos pontos de entrada de dados; e
3. empregar tecnologias que resolvem automaticamente certas situações perigosas.

Resposta a incidentes. O Google monitora uma variedade de canais de comunicação para incidentes de segurança, e o departamento de segurança do Google reagirá prontamente a incidentes conhecidos.

Tecnologias de criptografia. O Google disponibiliza criptografia de HTTPS, também chamada de “conexão TLS”. Os servidores do Google são compatíveis com troca de chaves criptográficas Diffie Hellman via curvas elípticas efêmeras assinadas com RSA e ECDSA. Esses métodos de perfect forward secrecy (PFS) ajudam a proteger o tráfego e minimizam o impacto de uma chave comprometida ou de uma inovação criptográfica.

2. Controles de Acesso e Local

(a) **Controles do local**.

Operação de segurança local de data centers. Os data centers do Google mantêm uma operação de segurança local responsável por todas as funções, 24 horas por dia, 7 dias por semana. A equipe da operação de segurança local monitora câmeras do circuito fechado de TV ("**CFTV**", na sigla em inglês) e todos os sistemas de alarme. Eles realizam rondas internas e externas regularmente no data center.

Procedimentos de acesso aos data centers. O Google mantém procedimentos formais para permitir o acesso físico aos data centers. Os data centers ficam em instalações que exigem acesso por chave eletrônica, com alarmes que são vinculados à operação de segurança local. Todas as pessoas que entram no data center são obrigadas a se identificar e mostrar um comprovante de identidade para a equipe de operações de segurança local. Somente funcionários, prestadores de serviços e visitantes autorizados têm permissão para entrar nos data centers. Somente funcionários e prestadores de serviços autorizados têm permissão para solicitar acesso por chave eletrônica a essas instalações. As solicitações de acesso por chave eletrônica precisam ser feitas com antecedência e por escrito e exigem autorização da equipe autorizada do data center. Todas as outras pessoas que precisam de acesso temporário devem: (i) receber aprovação prévia da equipe do data center e das equipes das áreas internas que querem visitar; (ii) identificar-se em todas as operações de segurança local; e (iii) apresentar um registro de acesso ao data center que identifique a pessoa como aprovada.

Dispositivos de segurança local dos data centers. Os data centers do Google utilizam uma chave eletrônica e um sistema biométrico para controle de acesso vinculado a um alarme do sistema. O sistema de controle de acesso monitora e registra a chave eletrônica de cada indivíduo e quando ele acessa as portas de perímetro, a área de envio/recebimento e outras áreas críticas. Atividades não autorizadas e tentativas frustradas de acesso são registradas pelo sistema de controle de acesso e investigadas, quando aplicável. O acesso autorizado às operações comerciais e aos data centers é restrito de acordo com as zonas e as responsabilidades profissionais do indivíduo. As portas corta-fogo nos data centers são equipadas com alarmes. Câmeras do CFTV ficam em operação nas partes interna e externa dos data centers. O posicionamento das câmeras foi efetivado para cobrir áreas estratégicas, incluindo, entre outras, o perímetro, as portas para o prédio dos data centers e as áreas de envio/recebimento. A equipe de operações de segurança local gerencia os equipamentos de monitoramento, gravação e controle do CFTV. Cabos seguros nas centrais de dados conectam os equipamentos do CFTV. Câmeras gravam o local por meio de filmadoras digitais 24 horas por dia, 7 dias por semana. Os registros de vigilância são mantidos por pelo menos sete dias, dependendo da atividade.

(b) **Controle de acesso**.

Equipe de segurança da infraestrutura. O Google tem e mantém uma política de segurança para sua equipe de segurança da infraestrutura e exige treinamento de segurança como parte do pacote de treinamento da equipe. A equipe de segurança da infraestrutura do Google é responsável pelo monitoramento contínuo dessa infraestrutura, pela análise dos Serviços de Operador e por responder a incidentes de segurança.

Gerenciamento de privilégios e controle de acesso. Os administradores e usuários do Cliente precisam ser autenticados por um sistema de autenticação ou por login único para poder acessar os Serviços de Operador.

Políticas e processos internos de acesso a dados — Política de acesso. As políticas e os processos internos de acesso a dados do Google são criados para evitar que pessoas não autorizadas e/ou sistemas tenham acesso aos sistemas usados para tratar dados pessoais. O Google busca criar sistemas para: (i) permitir que somente pessoas autorizadas tenham acesso aos dados que elas têm autorização para acessar; e (ii) garantir que os dados pessoais não possam ser lidos, copiados, alterados ou removidos sem autorização durante o tratamento e após a gravação. Os sistemas são desenvolvidos para detectar qualquer acesso inadequado. O Google utiliza um sistema de gerenciamento de acesso centralizado para controlar a liberação da

equipe aos servidores de produção e só a concede a um número limitado de pessoas autorizadas. O LDAP, o Kerberos e um sistema proprietário que utiliza certificados digitais são desenvolvidos para fornecer ao Google mecanismos de acesso seguros e flexíveis. Esses mecanismos são projetados para conceder somente direitos de acesso aprovado a hospedagens, registros, dados e informações de configuração do website. O Google exige o uso de códigos de usuários únicos, senhas fortes, autenticação de dois fatores e listas de acesso cuidadosamente monitoradas para minimizar a possibilidade de uso não autorizado de contas. A concessão ou modificação de direitos de acesso se baseia nas responsabilidades da função, nos requisitos das obrigações profissionais necessárias para realizar tarefas autorizadas e na necessidade de acesso da equipe autorizada. A concessão ou modificação de direitos de acesso também estará de acordo com as políticas e o treinamento de acesso a dados internos do Google. As aprovações são gerenciadas por ferramentas de fluxo de trabalho que mantêm registros de auditoria de todas as alterações. O acesso a sistemas é registrado para criar uma trilha de auditoria para prestação de contas. Sempre que as senhas são empregadas para autenticação (por exemplo, no login em estações de trabalho), são implementadas políticas de senha que seguem no mínimo as práticas padrão do setor. Esses padrões incluem restrições sobre reutilização e nível de segurança das senhas.

3. Dados

(a) **Armazenamento, isolamento e autenticação de dados.**

O Google armazena dados em um ambiente multilocatário em servidores do Google. Os dados, o banco de dados dos Serviços de Operador e a arquitetura do sistema de arquivos são replicados entre vários data centers espalhados em diversas localidades. O Google isola os dados de cada cliente de forma lógica. Um sistema de autenticação central é usado em todos os Serviços de Operador para aumentar a segurança uniforme dos dados.

(b) **Discos Desativados e orientação para a destruição de discos**.

Alguns discos que contêm dados podem apresentar problemas de desempenho, erros ou falhas de hardware que fazem com que eles sejam desativados ("**Disco Desativado**"). Todos os Discos Desativados são submetidos a uma série de processos de destruição de dados (as "**Orientações para a destruição de discos**") antes de deixar as instalações do Google para reutilização ou destruição. Os Discos Desativados são apagados em um processo de várias etapas e verificados por pelo menos dois avaliadores independentes. Os resultados da limpeza são registrados pelo número de série do Disco Desativado para rastreamento. Por fim, o Disco Desativado apagado é liberado para o inventário para reutilização e reimplementação. Se, devido a uma falha de hardware, o Disco Desativado não puder ser apagado, ele será armazenado em segurança até que possa ser destruído. Cada instalação é auditada regularmente para monitoramento da conformidade com as Orientações para Destruição de Dados.

4. Segurança dos Funcionários

Os funcionários do Google se comportam de maneira consistente com as orientações da empresa relativas a confidencialidade, ética nos negócios, uso adequado e padrões profissionais. O Google realiza investigações de histórico para contratação adequadas, dentro do legalmente permitido e de acordo com as leis trabalhistas locais e regulamentações aplicáveis.

Os funcionários do Google assinam um acordo de confidencialidade e confirmam o recebimento das políticas de privacidade e confidencialidade do Google e a conformidade com ambas. Os funcionários do Google recebem treinamento de segurança. Aqueles que lidam com Dados Pessoais do Cliente precisam satisfazer outros requisitos adequados à respectiva função. Os funcionários do Google não processam Dados Pessoais do Cliente sem autorização.

5. Segurança do Suboperador

Antes da integração dos Suboperadores, o Google realiza uma auditoria das práticas de segurança e privacidade dos Suboperadores para garantir que eles forneçam um nível de segurança e privacidade adequados ao acesso e ao escopo dos serviços que precisam prestar. Depois que o Google avalia os riscos apresentados pelo Suboperador, o Suboperador assinará contratos de segurança, confidencialidade e privacidade adequados, sempre sujeito aos requisitos definidos na Seção 11.3 (Requisitos para a Contratação de Suboperadores).

Apêndice 3: Termos Adicionais para Legislação Não Europeias de Proteção de Dados

Os Termos Adicionais para Legislação Não Europeias de Proteção de Dados complementam estes Termos de Processamento de Dados:

- Adendo do Provedor de Serviços da CCPA em privacy.google.com/businesses/processorterms/ccpa (1º de janeiro de 2020)

Termos de Processamento de Dados do Google Ads, versão 2.0

12 de agosto de 2020