Termos de Tratamento de Dados do Google Ads

O Google e a contraparte que aceita estes termos (o "**Cliente**") celebraram um contrato de prestação de Serviços de Operador (conforme periodicamente alterado, o "**Contrato**").

Estes Termos de Tratamento de Dados do Google Ads (juntamente com os apêndices, os "**Termos de Tratamento de Dados**") são celebrados pelo Google e pelo Cliente e complementam o Contrato. Estes Termos de Tratamento de Dados entrarão em vigor e substituirão quaisquer termos anteriormente aplicáveis relativos ao objeto em questão (incluindo quaisquer adendos ou alterações ao tratamento de dados com relação aos Serviços de Operador), a partir da data de Início da Vigência dos Termos.

Se você está aceitando estes Termos de Tratamento de Dados em nome do Cliente, você garante que: (a) tem plenos poderes legais para vincular o Cliente a estes Termos de Tratamento de Dados; (b) leu e entendeu estes Termos de Tratamento de Dados; e (c) aceita estes Termos de Tratamento de Dados, em nome do Cliente. Se você não tem poderes legais para vincular o Cliente, não aceite estes Termos de Tratamento de Dados.

1. Introdução

Estes Termos de Tratamento de Dados refletem o acordo celebrado entre as partes sobre os termos que regem o tratamento de determinados dados ao abrigo da Legislação Europeia em matéria de Proteção de Dados e de determinada Legislação Não Europeia em matéria de Proteção de Dados.

2. Definições e interpretação

2.1 Nestes Termos de Tratamento de Dados:

"**Autoridade Supervisora**" significa, conforme aplicável: (a) uma "autoridade supervisora" conforme definida no GDPR da UE; e/ou (b) o "Comissário" conforme definido no GDPR do Reino Unido e/ou na FDPA da Suíça.

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

"**Dados Pessoais do Cliente**" significa os dados pessoais tratados pelo Google em nome do Cliente no âmbito da prestação dos Serviços de Operador por parte do Google.

"**Data de 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 Tratamento de Dados antes ou nessa mesma data; ou

(b) a data em que o Cliente clicou para aceitar ou a date em que as partes, de outra forma, aceitaram estes Termos de Tratamento de Dados, se essa data for posterior a 25 de maio de 2018.

"**Documentação de Segurança**" significa o certificado emitido para a Certificação ISO 27001 e qualquer outra certificação ou documento de segurança que o Google possa disponibilizar relativamente aos Serviços de Operador.

"**EEE**" significa o Espaço Econômico Europeu.

"**Endereço de E-mail para Recebimento de Notificações**" significa o endereço de e-mail designado pelo Cliente, na interface do usuário dos Serviços de Operador ou em outros meios fornecidos pelo Google, para receber notificações da parte do Google relacionadas com estes Termos de Tratamento de Dados.

"**Entidade do Google**" significa a Google LLC (anteriormente chamada de "Google Inc."), a Google Ireland Limited ou qualquer outra entidade que controla direta ou indiretamente, é controlada ou está sob o controle comum da Google LLC.

"**FDPA da Suíça**" significa a Lei Federal de Proteção de Dados de 19 de junho de 1992 (Suíça).

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

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

"**GDPR da União Europeia**" significa o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

"**GDPR do Reino Unido**" significa o GDPR da UE conforme alterado e incorporado na legislação do Reino Unido, de acordo com os termos da Lei de Saída do Reino Unido da União Europeia de 2018 (UK European Union (Withdrawal) Act 2018), e a legislação secundária aplicável elaborada de acordo com essa lei.

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

"**Incidente com Dados**" significa uma violação de 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 com Dados" não incluem atividades ou tentativas malsucedidas que não comprometam 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.

"**Instruções**" tem o significado atribuído na Seção 5.2 (Instruções do Cliente).

"**Legislação Europeia**" significa, conforme aplicável: (a) a legislação da UE ou de estado-membro da UE (caso o GDPR da UE seja aplicável ao tratamento de Dados Pessoais do Cliente); e (b) a lei do Reino Unido ou de uma parte do Reino Unido (caso o GDPR do Reino Unido seja aplicável ao tratamento de Dados Pessoais do Cliente).

"**Legislação Europeia em matéria de Proteção de Dados**" significa, conforme aplicável, (a) o GDPR; e/ou (b) a FDPA da Suíça.

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

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

"**Novo Sub-Operador**" tem o significado atribuído na Seção 11.1 (Autorização para Engajamento de Sub-operadores).

"**País Adequado**" significa:

(a) para os dados tratados ao abrigo do GDPR da UE: o EEE ou um país ou território reconhecido por garantir um nível adequado de proteção de dados ao abrigo do GDPR da UE;

(b) para dados tratados ao abrigo do GDPR do Reino Unido: o Reino Unido ou um país ou território reconhecido por garantir um nível adequado de proteção de dados ao abrigo do GDPR do Reino Unido e da Lei de Proteção de Dados de 2018 do Reino Unido; e/ou

(c) para dados tratados ao abrigo da Lei Federal Suíça sobre Proteção de Dados [FDPA em inglês]: a Suíça ou um país ou território (i) incluído na lista de estados cuja legislação garante um nível adequado de proteção, conforme publicada pelo Comissário Federal de Proteção de Dados e Informação Suíço, ou (ii) reconhecido pelo Conselho Federal Suíço por garantir um nível adequado de proteção de dados de acordo com a FDPA da Suíça,

em todo o caso, com exceção daqueles que assentam em um regime de proteção de dados opcional.

"**Período de Vigência**" significa o período entre a Data de Início da Vigência dos Termos e o final do fornecimento dos Serviços de Operador por parte do Google ao abrigo do Contrato.

"**Produto Adicional**" significa 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.

"**SCCs**" significa as SCCs do Cliente e/ou as SCCs (Operador para Operador, Exportador do Google), conforme aplicável.

"**SCCs (Controlador para Operador)**" têm o significado definido em business.safety.google/adsprocessorterms/sccs/c2p.

"**SCCs (Operador para Controlador)**" têm o significado definido em business.safety.google/adsprocessorterms/sccs/p2c.

"**SCCs (Operador para Operador)**" têm o significado definido em business.safety.google/adsprocessorterms/sccs/p2p.

"**SCCs (Operador para Operador, Exportador do Google)**" têm o significado definido em business.safety.google/adsprocessorterms/sccs/p2p-intra-group.

"**SCCs de Clientes**" significa as SCCs Controlador para Operador, Operador para Controlador e/ou Operador para Operador, conforme aplicável.

"**Serviços de Operador**" significa os serviços aplicáveis listados em business.safety.google/adsservices.

"**Solução de Transferência Alternativa**" significa uma solução, diferente das SCCs (Cláusulas Contratuais Padrão), que permite a transferência lícita de dados pessoais para um país fora da UE ao abrigo da Legislação Europeia em matéria de Proteção de Dados como, por exemplo, um regime de proteção de dados

reconhecido por garantir que as entidades participantes prestam um nível adequado de proteção.

"**Sub-operadores**" significa os terceiros autorizados por estes Termos de Tratamento de Dados a ter acesso lógico e a tratar Dados Pessoais do Cliente a fim de fornecer partes dos Serviços de Operador e qualquer suporte técnico relacionado.

"**Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados**" significa os termos adicionais mencionados no Apêndice 3, que refletem o acordo entre as partes sobre os termos que regem o tratamento de determinados dados ao abrigo de determinada Legislação Não Europeia em matéria de Proteção de Dados.

2.2 Os termos "**controlador**", "**titular dos dados pessoais**", "**dados pessoais**", "**processamento**"/"**tratamento**" e "**operador**" usados nestes Termos de Tratamento de Dados terão os significados atribuídos a eles no GDPR. Os termos "**importador de dados**" e "**exportador de dados**" terão os significados atribuídos a eles nas SCCs aplicáveis.

2.3 As palavras "**incluir**" e "**incluindo**" significam "incluindo, mas não se limitando a". Todos os exemplos nestes Termos de Tratamento de Dados são ilustrativos, e não exemplos únicos de um conceito específico.

2.4 Qualquer referência a um regime legal, estatuto ou outro ato legislativo é uma referência a ele conforme periodicamente alterado ou promulgado.

2.5 Em caso de inconsistência entre a versão traduzida e a versão em inglês destes Termos de Tratamento de Dados, a versão em inglês terá precedência.

3. Duração destes Termos de Tratamento de Dados

Estes Termos de Tratamento de Dados entrarão em vigor na Data de Início da Vigência dos Termos. Não obstante a rescisão ou expiração do Contrato, estes Termos de Tratamento de Dados permanecerão em vigor até à eliminação de todos os Dados Pessoais do Cliente por parte do Google e expirarão automaticamente após esse fato, conforme descrito nesses Termos.

4. Aplicação destes Termos de Tratamento de Dados

4.1 **Aplicação da Legislação Europeia em matéria de Proteção de Dados**. As seções 5 (Tratamento de Dados) a 12 (Contato com o Google; Registros do Tratamento) serão empregadas somente na medida em que a Legislação Europeia em matéria de Proteção de Dados for aplicável ao tratamento dos Dados Pessoais do Cliente, inclusive se:

(a) o tratamento for realizado no contexto das atividades de um estabelecimento do Cliente situado no EEE ou no Reino Unido; e/ou

(b) os Dados Pessoais do Cliente forem dados pessoais referentes a titulares dos dados pessoais que se encontrem no EEE ou no Reino Unido e o tratamento se referir à oferta de bens ou serviços a esses titulares dos dados pessoais ou ao monitoramento do comportamento deles no EEE ou no Reino Unido.

4.2 **Aplicação aos Serviços de Operador**. Estes Termos de Tratamento de Dados só serão aplicados aos Serviços de Operador no âmbito dos quais as partes aceitaram estes Termos de Tratamento de Dados, por exemplo, (a) os Serviços de Operador para os quais o Cliente tenha aceitado estes Termos de Tratamento de

Dados ou (b) se o Contrato incorpora estes Termos de Tratamento de Dados por referência, os Serviços de Operador que são objeto do Contrato.

4.3 **Incorporação de Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados**. Os Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados complementam estes Termos de Tratamento de Dados.

5. Tratamento de Dados

5.1 **Funções e Conformidade Regulatória; Autorização**.

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

(a) o Apêndice 1 descreve o objeto 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 em matéria de Proteção de Dados;

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

(d) cada parte cumprirá as obrigações que para si decorrem ao abrigo da Legislação Europeia em matéria de Proteção de Dados no que diz respeito ao tratamento de Dados Pessoais do Cliente.

5.1.2 **Clientes Operadores**. Se o Cliente for um operador :

(a) o Cliente garante, de maneira contínua, que o controlador relevante autorizou: (i) as Instruções, (ii) a designação por parte do Cliente do Google como outro operador e (iii) o engajamento de Sub-operadores pelo Google, conforme descrito na Seção 11 (Sub-operadores);

(b) o Cliente encaminhará imediatamente ao controlador relevante qualquer notificação fornecida da parte do Google ao abrigo das Seções 5.4 (Notificações de Instrução), 7.2.1 (Notificações de Incidente), 11.4 (Oportunidade para se Opor a Alterações aos Sub-operadores) ou que se refira a SCCs; e

(c) o Cliente pode disponibilizar ao controlador relevante qualquer informação disponibilizada pelo Google ao abrigo das Seções 7.4 (Certificação de Segurança), 10.5 (Informações do Data Center) e 11.2 (Informações sobre Sub-operadores).

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) como especificado mais detalhadamente através do uso pelo Cliente dos Serviços de Operador (inclusive nas configurações e em outras funcionalidades dos Serviços de Operador) e em qualquer outro suporte técnico relacionado; (c) conforme documentado no formulário do Contrato, incluindo estes Termos de Tratamento de Dados; e (d) conforme documentado mais detalhadamente em quaisquer outras instruções por escrito fornecidas pelo Cliente e reconhecidas pelo Google como constituindo instruções para efeitos destes Termos de Tratamento de Dados (coletivamente, as "**Instruções**").

5.3 **Comprimento das Instruções pelo Google**. O Google cumprirá as Instruções, exceto quando tal seja proibido ao abrigo da Legislação Europeia.

5.4 **Notificações de Instrução**. O Google notificará imediatamente o Cliente se, na opinião do Google: (a) a Legislação Europeia proibir o Google de cumprir uma Instrução; (b) uma Instrução não estiver em conformidade com a Legislação Europeia em matéria de Proteção de Dados; ou (c) o Google não puder cumprir uma Instrução por qualquer motivo, a menos que essa notificação seja proibida pela Legislação Europeia. Esta Seção 5.4 (Notificações de Instrução) não afeta os direitos e as obrigações de nenhuma das partes previstos nas outras seções do Contrato.

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

6. Exclusão de Dados

6.1 **Exclusão Durante o Período de Vigência**.

6.1.1 **Serviços de Operador com Funcionalidades de Exclusão**. Se, durante o Período de Vigência:

(a) as funcionalidades dos Serviços de Operador incluirem a opção que permite ao Cliente excluir 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 esses Dados Pessoais do Cliente dos seus sistemas assim que razoavelmente possível e dentro de um período máximo de 180 dias, exceto se a Legislação Europeia exigir o armazenamento.

6.1.2 **Serviços de Operador sem Funcionalidades de Exclusão**. Durante o Período de Vigência, se as funcionalidades dos Serviços de Operador não incluirem a opção que permita ao Cliente excluir Dados Pessoais do Cliente, o Google cumprirá:

(a) com qualquer solicitação razoável do Cliente para agilizar essa exclusão, na medida em que isso seja possível dadas a natureza e as funcionalidades dos Serviços de Operador e exceto se a Legislação Europeia exigir o armazenamento; e

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

O Google poderá cobrar uma taxa (com base nos custos razoáveis que tenha) por qualquer exclusão de dados realizada 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 das taxas antes da exclusão dos dados em questão.

6.2 **Exclusão no Final do Período de Vigência**. O Cliente instrui o Google a excluir todos os Dados Pessoais do Cliente restantes (incluindo eventuais cópias) dos sistemas do Google no final do Período de Vigência, 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 a Legislação Europeia exigir o armazenamento.

7. Segurança dos Dados

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 acidental ou ilegal, conforme descrito no Apêndice 2 (as "**Medidas de Segurança**"). De acordo com o Apêndice 2, as Medidas de Segurança incluem ações para: (a) criptografar dados pessoais; (b) ajudar a garantir confidencialidade, integridade, disponibilidade e resiliência contínuas dos 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 degradação da segurança geral dos Serviços de Operador.

7.1.2 **Acesso e Conformidade**. O Google: (a) só autorizará os seus funcionários, contratados e Sub-operadores a acessar os Dados Pessoais do Cliente quando tal for estritamente necessário para cumprimento das Instruções; (b) tomará as providências cabíveis para garantir a conformidade com as Medidas de Segurança por parte dos funcionários, contratados e Sub-operadores na medida aplicável ao seu escopo de atuação; e (c) garantirá que todas as pessoas autorizadas a tratar Dados Pessoais do Cliente assumiram um compromisso de sigilo e confidencialidade ou têm uma obrigação legal adequada de confidencialidade.

7.1.3 **Assistência de Segurança do Google**. O Google, considerando a natureza do tratamento dos Dados Pessoais do Cliente e as informações que dispõe, ajudará o Cliente a garantir o cumprimento das obrigações do Cliente (ou, caso o Cliente seja um operador, as obrigações do controlador relevante) em matéria de segurança e de violações de dados pessoais, incluindo as obrigações do Cliente (ou, caso o Cliente seja um operador, as obrigações do controlador relevante) definidas nos Artigos 32.º a 34.º, inclusive, do GDPR, através:

(a) da implementação e manutenção de Medidas de Segurança de acordo com o previsto na Seção 7.1.1 (Medidas de Segurança do Google);

(b) do cumprimento dos termos previstos na Seção 7.2 (Incidentes com Dados); e

(c) da disponibilização ao Cliente da Documentação de Segurança de acordo com o previsto na Seção 7.5.1 (Análise da Documentação de Segurança) e das informações contidas nestes Termos de Tratamento de Dados.

7.2 **Incidentes com Dados**.

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

7.2.2 **Detalhes do Incidente com Dados**. As notificações feitas de acordo com o previsto na Seção 7.2.1 (Notificação de Incidentes) irão descrever: a natureza do Incidente com Dados, incluindo os recursos do Cliente afetados; as medidas que o Google tomou ou planeja tomar para resolver o Incidente com Dados e mitigar o potencial risco do mesmo; as medidas, se houver, que o Google recomenda que o Cliente tome para resolver o Incidente com Dados; e detalhes de um ponto de contato para a obtenção de mais informações. Se não for possível fornecer todas essas informações ao mesmo tempo, a notificação inicial do Google terá as informações disponíveis no momento, e mais detalhes serão fornecidos sem atrasos indevidos assim que estiverem disponíveis.

7.2.3 **Envio da Notificação**. O Google enviará a notificação sobre um Incidente com Dados para o Endereço de E-mail para Recebimento de Notificações ou, a

critério do Google (incluindo nos casos em que o Cliente não tenha fornecido esse endereço), por qualquer outro meio de comunicação direta (por exemplo, por telefone ou reunião presencial). O Cliente é a única parte responsável por fornecer o Endereço de E-mail para Recebimento de Notificações e garantir que esse endereço está atualizado e válido.

7.2.4 **Notificações a Terceiros**. O Cliente é a única parte responsável por cumprir o disposto nas leis em matéria de notificação de incidentes que sejam aplicáveis ao Cliente e por cumprir todas as obrigações de notificação a terceiros relacionadas com Incidentes com Dados.

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

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

7.3.1 **Responsabilidades de Segurança do Cliente**. O Cliente concorda que, sem prejuízo das obrigações do Google previstas nas Seções 7.1 (Medidas e Assistência de Segurança do Google) e 7.2 (Incidentes com Dados):

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

(i) pelo uso apropriado dos Serviços de Operador a fim de garantir um nível de segurança adequado ao risco no que diz respeito aos Dados Pessoais do Cliente; e

(ii) pela 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 os Dados Pessoais do Cliente que o Cliente pretenda armazenar ou transferir para fora dos sistemas do Google ou dos sistemas dos Sub-operadores do Google.

7.3.2 **Avaliação de Segurança do Cliente**. O Cliente reconhece e concorda que as Medidas de Segurança implementadas e mantidas pelo Google, nos termos previstos na Seção 7.1.1 (Medidas de Segurança do Google), oferecem um nível de segurança apropriado ao risco no que diz respeito aos Dados Pessoais do Cliente, considerando as tecnologias atuais, 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 as pessoas físicas.

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 **Análise da Documentação de Segurança**. Para demonstrar o cumprimento pelo Google das respetivas obrigações ao abrigo destes Termos de Tratamento de Dados, o Google disponibilizará a Documentação de Segurança para análise por parte 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 o cumprimento pelo Google das respetivas obrigações ao abrigo destes Termos de Tratamento de Dados, nos termos previstos na Seção 7.5.3 (Termos Comerciais Adicionais para Auditorias). Durante uma auditoria, o Google disponibilizará todas as informações necessárias para

demonstrar esse cumprimento e contribuirá com as auditorias conforme descrito na Seção 7.4 (Certificação de Segurança) e nesta Seção 7.5 (Análises e Auditorias de Conformidade).

(b) Se as SCCs forem aplicáveis, nos termos do disposto na Seção 10.2 (Transferências Europeias Restritas), o Google permitirá que o Cliente, ou um auditor terceirizado indicado por ele, conduza auditorias nos termos previstos nas SCCs e disponibilizará, durante a auditoria, todas as informações exigidas pelas SCCs, de acordo com o disposto na Seção 7.5.3 (Termos Comerciais Adicionais para Auditorias).

(c) O Cliente também pode realizar uma auditoria para verificar o cumprimento por parte do Google das respetivas obrigações ao abrigo destes Termos de Tratamento de Dados através da análise do certificado emitido para a Certificação ISO 27001 (que reflete o resultado de uma auditoria realizada por um auditor terceirizado).

7.5.3 **Termos Comerciais Adicionais para Auditorias**.

(a) O Cliente enviará ao Google todas as solicitações para a realização de uma auditoria ao abrigo da Seção 7.5.2(a) ou 7.5.2(b), nos termos previstos na Seção 12.1 (Contato com o Google).

(b) Depois de receber uma solicitação ao abrigo da Seção 7.5.3(a), o Google e o Cliente discutirão entre si e chegarão a um acordo prévio sobre a data de início, o escopo e duração razoáveis, bem como os controles de confidencialidade e segurança aplicáveis a qualquer auditoria prevista na Seção 7.5.2(a) ou 7.5.2(b).

(c) O Google poderá cobrar uma taxa, com base nos custos razoáveis que tenha, 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 antes da realização da auditoria em questão. O Cliente será responsável pelas taxas cobradas por um auditor terceirizado indicado por ele para executar a auditoria em questão.

(d) O Google poderá opor-se a qualquer auditor terceirizado indicado pelo Cliente para a realização das 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 por parte do Google exigirá que o Cliente indique outro auditor ou conduza ele próprio a auditoria.

(e) As disposições contidas nestes Termos de Tratamento de Dados não exigem que o Google divulgue ao Cliente ou ao auditor terceirizado ou permita que eles acessem a:

(i) dados de qualquer 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 vir a: (A) comprometer a segurança dos sistemas ou instalações de qualquer Entidade do Google; ou (B) fazer com que uma Entidade do Google incumpra as obrigações para ela decorrentes da Legislação Europeia em matéria 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 decorrentes da Legislação Europeia em matéria de Proteção de Dados.

8. Relatórios de Impacto e Consultas

O Google (levando em conta a natureza do tratamento e as informações disponíveis para o Google) auxiliará o Cliente a garantir o cumprimento das obrigações do Cliente (ou, caso o Cliente seja um operador, das obrigações do controlador relevante) em matéria de relatórios de impacto à proteção de dados e consulta prévia, incluindo, se aplicável, as obrigações do Cliente ou do controlador relevante previstas nos Artigos 35.º e 36.º do GDPR, através do:

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

(b) fornecimento das informações contidas no Contrato (incluindo estes Termos de Tratamento 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 do tratamento de Dados Pessoais do Cliente (por exemplo, materiais da Central de Ajuda).

9. Direitos do Titular dos Dados

9.1 **Respostas a Solicitações dos Titulares dos Dados**. Se o Google receber uma solicitação de um titular dos dados relativamente a Dados Pessoais do Cliente, o Cliente autoriza o Google a (e o Google desde já notifica o Cliente que irá):

(a) responder diretamente à solicitação do titular dos dados de acordo com a funcionalidade padrão da Ferramenta do Titular dos Dados (quando a solicitação tenha sido feita através dessa ferramenta); ou

(b) aconselhar o titular dos dados a enviar a sua solicitação para o Cliente, ficando o Cliente responsável por dar resposta à solicitação (quando a solicitação não tenha sido feita através de uma Ferramenta dos Titulares dos Dados).

9.2 **Assistência por parte do Google a Solicitações dos Titulares dos Dados**. O Google ajudará o Cliente a cumprir as respetivas obrigações (ou, se o Cliente for um operador, as obrigações do controlador relevante) previstas no Capítulo III do GDPR no sentido de responder às solicitações para exercício dos direitos dos titulares dos dados, tendo em conta, em todo o caso, a natureza do tratamento dos Dados Pessoais do Cliente e, se aplicável, o disposto no Artigo 11.º do GDPR, através:

(a) do fornecimento da funcionalidade dos Serviços de Operador;

(b) do cumprimento dos compromissos definidos na Seção 9.1 (Respostas a Solicitações dos Titulares dos Dados); e

(c) da disponibilização das Ferramentas dos Titulares dos Dados, se aplicáveis aos Serviços de Operador.

9.3 **Retificação**. Se o Cliente tomar conhecimento de que os Dados Pessoais do Cliente estão incorretos ou desatualizados, ele será responsável por retificar ou excluir esses dados, se tal for exigido pela Legislação Europeia em matéria de Proteção de Dados, usando, inclusive, a funcionalidade dos Serviços de Operador (quando a mesma se encontrar disponível).

10. Transferências de Dados

10.1 **Instalações de Armazenamento e Tratamento de Dados**. O Google pode tratar Dados Pessoais do Cliente em qualquer país em que ele ou qualquer Sub-operador relevante tenha instalações, sujeito ao restante desta Seção 10 (Transferências de Dados).

10.2 **Transferências Europeias Restritas**. As partes reconhecem que a Legislação Europeia em matéria de Proteção de Dados não exige as SCCs nem uma Solução de Transferência Alternativa para tratar Dados Pessoais do Cliente em um País Adequado ou para transferir Dados Pessoais do Cliente para um País Adequado. Se os Dados Pessoais do Cliente forem transferidos para qualquer outro país e a Legislação Europeia em matéria de Proteção de Dados se aplicar às transferências ("**Transferências Europeias Restritas**"):

(a) caso o Google adote uma Solução de Transferência Alternativa para as Transferências Europeias Restritas, o Google informará o Cliente da solução relevante e garantirá que as Transferências Europeias Restritas em questão são feitas de acordo com essa mesma solução; e/ou

(b) caso o Google não tenha adotado, ou tenha informado o Cliente de que não iria mais adotar uma Solução de Transferência Alternativa para as Transferências Europeias Restritas:

(i) se o endereço do Google estiver em um País Adequado:

(A) as Cláusulas Contratuais Padrão (ou SCCs em inglês) (Operador para Operador, Exportador do Google) serão aplicáveis relativamente a essas mesmas Transferências Europeias Restritas do Google para Sub-operadores; e

(B) além disso, se o endereço do Cliente não for em um País Adequado, as SCCs (Operador para Controlador) serão aplicáveis relativamente às Transferências Europeias Restritas entre o Google e o Cliente (independentemente de o Cliente ser um controlador e/ou um operador); ou

(ii) se o endereço do Google não estiver em um País Adequado, as SCCs (Controlador para Operador) e/ou as SCCs (Operador para Operador) serão aplicáveis (consoante o Cliente seja um controlador e/ou um operador) relativamente às Transferências Europeias Restritas em questão entre o Cliente e o Google.

10.3 **Informações e Medidas Complementares**. O Google fornecerá ao Cliente informações relevantes para as Transferências Europeias Restritas, incluindo informações sobre medidas complementares para a proteção dos Dados Pessoais do Cliente, conforme descrito na Seção 7.5.1 (Análise da Documentação de Segurança), no Apêndice 2 (Medidas de Segurança) e outros materiais relativos à natureza dos Serviços de Operador e do tratamento de Dados Pessoais do Cliente (por exemplo, artigos da Central de Ajuda).

10.4 **Rescisão**. Se o Cliente concluir, com base no seu uso atual ou pretendido dos Serviços de Operador, que a Solução de Transferência Alternativa e/ou as SCCs, conforme aplicável, não fornecem um nível de proteção adequada para os Dados Pessoais do Cliente, poderá o Cliente rescindir unilateralmente o Contrato com efeitos imediatos, mediante notificação por escrito ao Google.

10.5 **Informações do Data Center**. As informações sobre os locais onde estão instalados os data centers do Google estão disponíveis em www.google.com/about/datacenters/locations/.

11. Sub-operadores

11.1 **Autorização para Engajamento de Sub-operadores**. O Cliente autoriza especificamente o engajamento, como Sub-operadores, das entidades que, na Data de Início da Vigência dos Termos, se encontram listadas no URL especificado na Seção 11.2 (Informações sobre Sub-operadores). Além disso, sem prejuízo do disposto na Seção 11.4 (Oportunidade para se Opor a Alterações aos Sub-operadores), o Cliente autoriza, de modo geral, o engajamento de outros terceiros como Sub-operadores ("**Novos Sub-operadores**").

11.2 **Informações sobre Sub-operadores**. As informações relativas aos Sub-operadores estão disponíveis em business.safety.google/adssubprocessors.

11.3 **Requisitos para o Engajamento de Sub-operadores**. Ao engajar qualquer Sub-operador, o Google:

(a) garantirá, através de um contrato escrito, que:

(i) o Sub-operador só acessa e utiliza os Dados Pessoais do Cliente na medida do necessário para cumprir as obrigações subcontratadas ao mesmo, e o faz em conformidade com o Contrato (incluindo estes Termos de Tratamento de Dados); e

(ii) se o tratamento de Dados Pessoais do Cliente estiver sujeito à Legislação Europeia em matéria de Proteção de Dados, o Sub-operador fica sujeito às obrigações em matéria de proteção de dados previstos nestes Termos de Tratamento de Dados (conforme referido no Artigo 28(3) do GDPR, se aplicável); e

(b) permanecerá totalmente responsável por todas as obrigações subcontratadas e por todos os atos e omissões do Sub-operador.

11.4 **Oportunidade para se Opor a Alterações aos Sub-operadores**.

(a) Quando um novo Sub-operador for engajado durante o Período de Vigência, o Google informará ao Cliente do engajamento (incluindo o nome e a localização do respetivo Sub-operador e as atividades que ele realizará), pelo menos 30 dias antes de o Novo Sub-operador tratar quaisquer Dados Pessoais do Cliente, através do envio de um e-mail para o Endereço de E-mail para Recebimento de Notificações.

(b) O Cliente poderá opor-se a qualquer novo Sub-operador rescindindo unilateralmente o Contrato com efeitos imediatos, mediante notificação por escrito ao Google, desde que o Cliente envie essa notificação em um prazo de até 90 dias após ter sido informado sobre o engajamento do novo Sub-operador, nos termos previstos na Seção 11.4(a).

12. Contato com o Google; Registros do Tratamento

12.1 **Contato com o Google**. O Cliente pode entrar em contato com o Google relativamente ao exercício dos seus direitos previstos nestes Termos de Processamento de Dados através dos meios descritos em privacy.google.com/businesses/processorsupport ou de quaisquer outros meios que possam ser periodicamente disponibilizados pelo Google. O Google fornecerá assistência imediata e razoável para responder às dúvidas do Cliente recebidas por esses meios e que sejam referentes ao tratamento de Dados Pessoais do Cliente no âmbito do Contrato.

12.2 **Registros do Tratamento pelo Google**. O Google manterá uma documentação apropriada das suas atividades de tratamento, conforme exigido pelo GDPR. O

Cliente reconhece que, de acordo com o GDPR, o Google está obrigado a: (a) coletar e manter registros de determinadas informações, incluindo: (i) o nome e os 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 oficial de proteção de dados desse operador ou controlador, e (ii) se aplicável ao abrigo das SCCs do Cliente, a Autoridade Supervisora do Cliente; e a (b) disponibilizar essas informações a qualquer Autoridade Supervisora. Da mesma forma, o Cliente, quando solicitado e se aplicável, fornecerá essas informações ao Google através do interface do usuário dos Serviços de Operador ou através de qualquer outro meio que possa ser disponibilizado pelo Google e usará esse interface ou tais outros meios para garantir que todas as informações fornecidas sejam mantidas corretas e atualizadas.

12.3 **Solicitações de Controladores**. Se o Google receber uma solicitação ou instrução através dos meios descritos na Seção 12.1 (ou através de qualquer outro meio) de um terceiro que se apresente como controlador dos Dados Pessoais do Cliente, o Google orientará o terceiro a entrar em contato com o Cliente.

13. Responsabilidade

Se o Contrato for regido pela legislação de:

(a) um estado dos Estados Unidos da América, sem prejuízo de qualquer disposição no Contrato, a responsabilidade total de qualquer uma das partes em relação à outra parte decorrente ou relacionada com estes Termos de Tratamento de Dados será limitada ao valor monetário máximo ou ao valor baseado em pagamento a que a responsabilidade dessa parte está limitada ao abrigo do Contrato, não se aplicando, portanto, nenhuma exclusão de pedidos de indenização da limitação de responsabilidade prevista no Contrato a pedidos de indenização efetuados no âmbito do Contrato ao abrigo da Legislação Europeia em matéria de Proteção de Dados ou da Legislação Não Europeia em matéria de Proteção de Dados; ou

(b) uma jurisdição que não seja um estado dos Estados Unidos da América, a responsabilidade das partes decorrente ou relacionada com estes Termos de Tratamento de Dados estará sujeita às exclusões e limitações de responsabilidade previstas no Contrato.

14. Efeitos destes Termos de Tratamento de Dados

14.1 **Ordem de Precedência**. Em caso de qualquer conflito ou inconsistência entre as SCCs do Cliente, os Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados, as restantes disposições destes Termos de Tratamento de Dados e/ou as restantes disposições do Contrato, será aplicada a seguinte ordem de precedência:

(a) as SCCs do Cliente (se aplicável);

(b) os Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados (se aplicável);

(c) as restantes disposições destes Termos de Tratamento de Dados; e

(d) as restantes disposições do Contrato.

Sujeito às alterações introduzidas por estes Termos de Tratamento de Dados, o Contrato permanece em vigor e a produzir efeitos.

14.2 **Não introdução de alterações às SCCs**. O Contrato (incluindo estes Termos de Tratamento de Dados) não tem o objetivo de alterar ou contradizer as SCCs nem de prejudicar os direitos ou as liberdades fundamentais dos titulares dos dados previstos na Legislação Europeia em matéria de Proteção de Dados.

14.3 **Não Produção de Efeitos sobre os Termos Aplicáveis a Controladores**. Estes Termos de Tratamento de Dados não afetarão os termos independentes celebrados entre o Google e o Cliente que reflitam uma relação controlador-controlador para um serviço diferente dos Serviços de Operador.

14.4 **SCCs do Reino Unido preexistentes**. A partir de 21 de setembro de 2022, ou da data de entrada em vigor do Contrato, consoante a que ocorrer em último lugar, aplicam-se os termos suplementares das SCCs às transferências realizadas ao abrigo do GDPR do Reino Unido. Estes substituirão e rescindirão todas as cláusulas contratuais padrão aprovadas ao abrigo do GDPR do Reino Unido e da Lei da Proteção de Dados de 2018 anteriormente celebrados pelo Cliente e pelo Google ("SCCs do Reino Unido preexistentes"). Esta Seção 14.4 (SCCs do Reino Unido preexistentes) não afetará os direitos das partes nem quaisquer direitos do titular dos dados que possam ter sido adquiridos ao abrigo das SCCs do Reino Unido preexistentes durante a vigência das mesmas.

15. Alterações a estes Termos de Tratamento de Dados

15.1 **Alterações de URLs**. O Google pode periodicamente alterar qualquer URL mencionado nestes Termos de Tratamento de Dados e o conteúdo desse mesmo URL. No entanto, o Google só pode mudar:

(a) as SCCs de acordo com o disposto nas Seções 15.2 (b) - 15.2 (d) (Alterações a estes Termos de Tratamento de Dados) ou para incorporar novas versões das SCCs que possam ser adotadas de acordo com a Legislação Europeia em matéria de Proteção de Dados, sempre de maneira que não afete a validade das SCCs ao abrigo da Legislação Europeia em matéria de Proteção de Dados; e

(b) a lista de potenciais Serviços de Operador disponível em business.safety.google/adsservices: (i) para refletir uma mudança no nome de um serviço; (ii) para adicionar um novo serviço; ou (iii) para remover um serviço (ou uma funcionalidade de um serviço) quando: (x) todos os contratos para a prestação desse serviço forem rescindidos; ou (y) o Google tenha autorização da parte do Cliente; ou (z) o serviço, ou uma determinada funcionalidade do serviço, foi recategorizado(a) como um serviço de controlador.

15.2 **Alterações aos Termos de Tratamento de Dados**. O Google poderá modificar estes Termos de Tratamento de Dados se a alteração:

(a) for expressamente permitida por estes Termos de Tratamento de Dados, inclusive conforme descrito na Seção 15.1 (Alterações de URLs);

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

(c) for necessária para cumprir com o disposto numa lei ou regulamento aplicável, numa ordem judicial ou numa orientação expedida por um órgão regulador ou agência do governo, ou para refletir a adoção por parte do Google de uma Solução de Transferência Alternativa; ou

(d) não: (i) resultar em degradação da segurança geral dos Serviços de Operador; (ii) ampliar o escopo nem remover qualquer restrição sobre, (x) no caso dos Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados, os direitos do Google de usar ou, de outra forma, tratar os dados objeto dos Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados ou (y) no caso das restantes disposições destes Termos de Tratamento de Dados, o tratamento de Dados Pessoais do Cliente por parte do Google, conforme descrito na Seção 5.3 (Comprimento das Instruções pelo Google); e (iii) tiver um impacto negativo significativo sobre os direitos do Cliente ao abrigo destes Termos de Tratamento de Dados, conforme

razoavelmente determinado pelo Google.

15.3 **Notificação de Alterações**. Caso o Google tenha intenção de alterar estes Termos de Tratamento de Dados nos termos previstos na Seção 15.2(c) ou (d), o Google informará o Cliente pelo menos 30 dias antes de a alteração entrar em vigor, ou em um período menor, quando tal seja exigido por lei ou regulamento aplicável, por uma ordem judicial ou orientação expedida por um regulador ou órgão do governo. Isso precisa ser feito (a) enviando uma mensagem para o Endereço de E-mail para Recebimento de Notificações ou (b) alertando o Cliente através da interface do usuário dos Serviços de Operador. Caso o Cliente se oponha a qualquer uma dessas alterações, ele poderá rescindir unilateralmente o Contrato, com efeitos imediatos, enviando uma notificação por escrito ao Google até 90 dias após ter sido informado de tal alteração.

Apêndice 1: Objeto e Detalhes do Tratamento de Dados

Objeto

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

Duração do Tratamento

O Período de Vigência, mais o tempo entre o fim desse período e a data de exclusão de todos os Dados Pessoais do Cliente pelo Google de acordo com estes Termos de Tratamento 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 Tratamento de Dados. O tratamento inclui a coleta, registro, organização, estruturação, armazenamento, alteração, recuperação, uso, divulgação, combinação, exclusão e destruição, conforme aplicável aos Serviços de Operador e às Instruções.

Tipos de dados pessoais

Os Dados Pessoais do Cliente podem incluir os tipos de dados pessoais descritos em business.safety.google/adsservices.

Categorias de titulares dos dados

Os Dados Pessoais do Cliente serão referentes às seguintes categorias de titulares dos dados:

- titulares dos dados sobre os quais o Google coleta dados pessoais ao prestar os Serviços de Operador e/ou
- titulares dos dados cujos dados pessoais são transferidos para o Google no âmbito dos Serviços de Operador, quer pelo Cliente, por instrução dele ou em nome dele.

Dependendo da natureza dos Serviços de Operador, esses titulares dos dados podem incluir indivíduos: (a) a quem tenha sido, ou venha a ser direcionada publicidade on-line; (b) que tenham visitado websites ou aplicativos específicos no âmbito dos quais o Google presta os Serviços de Operador; e/ou (c) que sejam clientes ou usuários dos produtos ou serviços do Cliente.

Apêndice 2: Medidas de Segurança

A partir da Data de Início da Vigência dos Termos, o Google implementará e manterá as Medidas de Segurança definidas neste Apêndice 2. O Google pode atualizar ou modificar essas Medidas de Segurança periodicamente, desde que essas atualizações e modificações não resultem na degradação 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 de produção em data centers fisicamente protegidos.

Redundância. Os sistemas da infraestrutura foram criados para eliminar pontos únicos de falha e minimizar o impacto de riscos ambientais previsíveis. Circuitos duplos, interruptores, redes ou outros dispositivos necessários ajudam a proporcionar essa redundância. 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 ambientais têm procedimentos de manutenção preventiva documentados 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 um processo padrão, de acordo com procedimentos documentados.

Energia. Os sistemas de energia elétrica dos data centers são desenvolvidos para serem redundantes 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 como, por exemplo, baterias de fonte de alimentação ininterrupta (UPS, na sigla em inglês), que oferecem proteção elétrica consistentemente fiável durante blecautes parciais da concessionária de serviços públicos, blecautes, sobretensão/subtensão e condições de frequência fora da tolerância. Se a energia for interrompida, a alimentação de reserva fornecerá energia momentânea ao data center, na capacidade total, por um período de até 10 minutos, até que os sistemas de geradores de reserva sejam acionados. Os geradores de reserva 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 dos Servidores. Os servidores do Google usam sistemas operacionais robustos que são customizados para as necessidades exclusivas dos servidores da atividade. Os dados são armazenados através de algoritmos exclusivos para aumentar a segurança e redundância dos dados. O Google emprega um processo de revisão de código para aumentar a segurança do código usado para prestar os Serviços de Operador e melhorar os produtos de segurança em ambientes de produção.

Continuidade do Negócio. O Google replica dados em vários sistemas para ajudar a protegê-los contra a sua destruição ou perda acidental. O Google desenvolveu, e planeja e testa regularmente os programas para recuperação de desastres/planejamento de continuidade do negócio.

Tecnologias de Criptografia. As políticas de segurança do Google exigem a criptografia em repouso para todos os dados do usuário, incluindo os dados pessoais. Os dados são geralmente criptografados em vários níveis na pilha de armazenamento de produção do Google em data centers, inclusive no nível do hardware, sem necessidade de nenhuma ação por parte dos clientes. O uso de várias camadas de criptografia oferece proteção redundante aos dados e permite que o Google selecione a abordagem ideal com base nos requisitos do aplicativo. Todos os dados pessoais são criptografados quando são armazenados, geralmente usando AES256. O Google usa bibliotecas criptográficas comuns que incorporam o módulo FIPS 140-2 do Google para implementar a criptografia de forma consistente em todos os Serviços de Operador.

(b) **Redes e Transmissão**.

Transmissão de Dados. Os data centers são geralmente conectados através de links privados de alta velocidade que proporcionam uma transferência de dados segura e rápida entre os data centers. 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 através de protocolos padrão da Internet.

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

Detecção de Intrusões. A detecção de intrusões tem o objetivo de fornecer informações sobre atividades de ataque em andamento e informações adequadas para responder a incidentes. A detecção de intrusão do Google consiste em:

1. Controlar de forma rigorosa o tamanho e a composição da superfície de ataque do Google com medidas preventivas;
2. Empregar controles de detecção inteligentes 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. O pessoal de segurança do Google reagirá prontamente a incidentes identificados.

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

2. Controles de Acesso e do Local

(a) **Controles do Local**.

Operação de Segurança Local nos Data Centers. Os data centers do Google mantêm uma operação de segurança local responsável por todas as funções físicas de segurança do data center, 24 horas por dia, 7 dias por semana. A equipe da operação de segurança local monitora câmeras do circuito fechado de TV (ou CCTV, na sigla em inglês) e todos os sistemas de alarme. A equipe da operação de segurança local realiza 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 estão alojados em instalações que exigem acesso através de cartão eletrônico, com alarmes que estão ligados 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, contratados e visitantes autorizados têm permissão para entrar nos data centers. Somente funcionários e contratados autorizados têm permissão para solicitar acesso por cartão eletrônico a essas instalações. As solicitações de acesso por cartão eletrônico 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 ao data center devem: (i) obter autorização prévia da equipe do data center específico 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 empregam um sistema de cartão eletrônico e um sistema de controle de acesso

biométrico que está ligado 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 do perímetro, a área de envio/recebimento e outras áreas críticas. As atividades não autorizadas e as tentativas frustradas de acesso são registradas pelo sistema de controle de acesso e investigadas, quando adequado. O acesso autorizado às operações comerciais e aos data centers é restrito de acordo com as zonas e as responsabilidades inerentes à função da pessoa em questão. As portas corta-fogo nos data centers estão equipadas com alarmes. As câmeras de CCTV estão em funcionamento tanto dentro como fora dos data centers. O posicionamento das câmeras foi pensado para cobrir áreas estratégicas, incluindo, entre outras, o perímetro, as portas de acesso ao edifício dos data centers e as áreas de envio/recebimento. A equipe de operações de segurança local gerencia os equipamentos de monitoramento, gravação e controle de CCTV. O equipamento de CCTV é conectado por cabos fixos instalados ao longo dos data centers. As câmeras gravam o local 24 horas por dia, 7 dias por semana por meio de filmadoras digitais. 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 seu pessoal 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 devem se autenticar através de um sistema de autenticação central ou por logon único para poder usar 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 e/ou sistemas não autorizados tenham acesso aos sistemas usados para tratar dados pessoais. O Google pretende conceber os seus sistemas de forma a: (i) permitir que apenas 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 nem removidos sem autorização durante o tratamento, uso e posterior gravação. Os sistemas são desenvolvidos para detectar qualquer acesso indevido. O Google emprega um sistema centralizado de gerenciamento de acesso para controlar o acesso da equipe aos servidores de produção e só o concede a um número limitado de pessoas autorizadas. O LDAP, o Kerberos e um sistema próprio e exclusivo que utiliza certificados foram desenvolvidos para fornecer ao Google mecanismos de acesso seguros e flexíveis. Estes mecanismos foram concebidos para só conceder os direitos de acesso aprovados aos anfitriões, registros, dados e informações de configuração do site. 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 inerentes às funções da equipe autorizada, nos requisitos necessários para a execução de tarefas autorizadas e no princípio da necessidade de saber. A concessão ou modificação de direitos de acesso também precisa estar de acordo com as políticas e o treinamento em matéria da 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 efeitos de responsabilização. Sempre que as senhas são empregadas para autenticação (por exemplo, no login em estações de trabalho), são implementadas políticas de senha que seguem pelo menos as práticas padrão do setor. Esses padrões incluem restrições sobre a reutilização e o nível de segurança das senhas.

3. Dados

(a) **Armazenamento, Isolamento e Autenticação de Dados**.

O Google armazena dados em um ambiente multilocatário em servidores pertencentes ao Google. Os dados, o banco de dados dos Serviços de Operador e a arquitetura do sistema de arquivos são replicados em vários data centers espalhados em diversas áreas geográficas. O Google isola os dados de cada cliente de

forma lógica. É usado um sistema de autenticação central em todos os Serviços de Operador para aumentar a segurança uniforme dos dados.

(b) **Discos Desativados e Orientações 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 Dados**") 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 para efeitos de rastreamento pelo número de série do Disco Desativado. 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 a Destruição de Dados.

(c) **Dados Pseudonimizados**.

Os dados de publicidade on-line são geralmente associados a identificadores on-line que, por si só, são considerados "pseudonimizados", ou seja, não podem ser atribuídos a um indivíduo específico sem o uso de informações adicionais. O Google dispõe de um conjunto robusto de políticas e controles técnicos e organizacionais em vigor para garantir a separação entre dados pseudonimizados e informações de identificação pessoal do usuário, ou seja, dados que possam ser usados para identificar ou contatar diretamente ou localizar com precisão um indivíduo, como é o caso dos dados da Conta do Google do usuário. As políticas do Google só permitem fluxos de informações entre dados pseudonimizados e dados pessoais em circunstâncias estritamente limitadas.

(d) **Análises de lançamento**.

O Google conduz análises antes do lançamento de novos produtos e funcionalidades. O que inclui uma análise de privacidade realizada por engenheiros de privacidade especialmente treinados. Nas análises de privacidade, os engenheiros de privacidade garantem que todas as políticas e diretrizes aplicáveis do Google foram seguidas, incluindo, mas não se limitando as políticas relacionadas à pseudonimização e à retenção e exclusão de dados.

4. Segurança da Equipe

A equipe do Google deve se comportar de maneira consistente com as orientações da empresa em matéria de confidencialidade, ética nos negócios, uso adequado e padrões profissionais. O Google realiza verificações de antecedentes razoavelmente apropriadas na medida do legalmente permitido e de acordo com a legislação trabalhista local e os regulamentos estatutários aplicáveis.

A equipe deve assinar um acordo de confidencialidade e confirmar o recebimento das Políticas de Privacidade e Confidencialidade do Google e que irá cumprir com elas. A equipe recebe treinamento de segurança. Aqueles que lidam com Dados Pessoais do Cliente precisam satisfazer outros requisitos adequados à respetiva função. A equipe do Google não tratará Dados Pessoais do Cliente sem autorização.

5. Segurança do Sub-operador

Antes da integração dos Sub-operadores, o Google realiza uma auditoria às práticas de segurança e privacidade dos Sub-operadores para garantir que eles fornecem um nível de segurança e privacidade adequado ao acesso deles a dados e ao escopo dos serviços que precisam prestar. Depois que o Google avalia os riscos apresentados pelo Sub-operador, este precisa assinar termos contratuais em matéria de segurança, confidencialidade e privacidade adequados, sempre sujeitos aos requisitos definidos na Seção 11.3 (Requisitos para o Engajamento de Sub-operadores).

Apêndice 3: Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados

Os Termos Adicionais para Legislação Não Europeia em matéria de Proteção de Dados complementam estes Termos de Tratamento de Dados:

- Adendo do Provedor de Serviços ao abrigo da CCPA disponível em business.safety.google/adsprocessorterms/ccpa/ (datado de 1 de janeiro de 2020)
- Adendo do Operador ao abrigo da LGPD em business.safety.google/adsprocessorterms/lgpd/ (datado de 16 de agosto de 2020)

Termos de Tratamento de Dados do Google Ads, versão 4.0

21 de setembro de 2022

Versões anteriores

- 27 de setembro de 2021
- 16 de agosto de 2020
- 12 de agosto de 2020
- 1º de janeiro de 2020
- 31 de outubro de 2019
- 12 de outubro de 2017