Aditivo sobre Tratamento de Dados do Cloud (Parceiros)

Este Aditivo sobre Tratamento de Dados do Cloud (incluindo os anexos dele, o *Aditivo*) é incorporado ao Contrato (conforme definido abaixo) celebrado entre o Google e o Parceiro. Este Aditivo era denominado "Termos de Segurança e Tratamento de Dados" para o Google Cloud Platform e "Aditivo sobre Tratamento de Dados" ou "Termos de Segurança e Tratamento de Dados" para o Looker (original) ou para os Serviços de SecOps do Google.

Termos Gerais

1. Visão Geral

Este Aditivo descreve as obrigações das partes, inclusive nos termos das leis aplicáveis de privacidade, segurança e proteção de dados, com relação ao tratamento e à segurança dos Dados do Parceiro. Este Aditivo começa a valer a partir do Início da Vigência do Aditivo (conforme definida abaixo) e substituirá quaisquer termos anteriormente aplicáveis ao tratamento e à segurança dos Dados do Parceiro. Os termos com iniciais maiúsculas usados, mas não definidos neste Aditivo, têm os significados atribuídos a eles no Contrato.

2. Definições

2.1 Neste Aditivo:

- *Início da Vigência do Aditivo* significa a data em que o Parceiro aceitou este Aditivo ou em que as partes, por outro meio, acordaram quanto à vigência dele.
- *Controles de Segurança Adicional* refere-se a recursos, funcionalidades e controles de segurança que o Parceiro pode utilizar a critério exclusivo dele, incluindo o Admin Console, criptografia, registro e monitoramento, gerenciamento de identidade e acesso, verificação de segurança e firewalls.
- *Contrato* significa o instrumento pelo qual o Google concordou em oferecer os Serviços aplicáveis ao Parceiro.
- *Lei de Privacidade Aplicável* indica qualquer lei ou regulamento estadual, provincial, nacional, federal, da União Europeia ou de outra jurisdição, relacionado à privacidade, à segurança ou à proteção de dados, conforme aplicável ao tratamento dos Dados Pessoais do Parceiro. Para maior clareza, as Leis de Privacidade Aplicáveis incluem, mas não estão limitadas às leis mencionadas no Apêndice 3 (Leis de Privacidade Específicas).

- *Serviços Auditados* refere-se aos Serviços vigentes que fazem parte do escopo da certificação ou do relatório correspondente em https://cloud.google.com/security/compliance/services-in-scope. O Google não poderá remover Serviços desse endereço, a menos que tenham sido descontinuados de acordo com o Contrato.

- *Certificações de Conformidade* tem o significado atribuído na Seção 7.4 (Certificações de Conformidade e Relatórios SOC).

- *Incidente de Dados* refere-se a uma violação de segurança do Google que gera destruição, perda, alteração, divulgação não autorizada ou acesso ilícitos ou acidentais aos Dados do Parceiro em sistemas gerenciados ou controlados pelo Google.

- *EMEA* significa Europa, Oriente Médio e África.

- *GDPR da União Europeia* refere-se ao Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, que aborda a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação dessas informações, revogando a Diretiva 95/46/CE.

- *Lei Europeia de Proteção de Dados* indica, conforme aplicável: (a) o GDPR; ou (b) a FADP da Suíça.

- *Legislação Europeia* significa, conforme aplicável: (a) a legislação da União Europeia ou de seus Estados-Membros (caso o GDPR da UE se aplique ao tratamento dos Dados Pessoais do Parceiro); (b) a legislação do Reino Unido ou de parte do Reino Unido (caso o GDPR do Reino Unido se aplique ao tratamento dos Dados Pessoais do Parceiro); ou (c) a legislação suíça (caso a FADP da Suíça se aplique ao tratamento dos Dados Pessoais do Parceiro).

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

- *Auditor Terceirizado do Google* refere-se a um auditor terceirizado, qualificado, independente e indicado pelo Google, com identidade atual a ser revelada ao Parceiro pelo Google.

- *Instruções* tem o significado atribuído na Seção 5.2 (Conformidade com as Instruções do Parceiro).

- *Endereço de E-mail para Notificação* refere-se aos endereços indicados pelo Parceiro no Admin Console ou no Formulário de Pedido para receber determinadas notificações do Google.

- *Usuários Finais do Parceiro* tem o significado atribuído no Contrato ou, caso não haja tal definição, o significado atribuído a "Usuários Finais" no Contrato.

- *Dados Pessoais do Parceiro* refere-se às informações contidas nos Dados do Parceiro, incluindo categorias especiais de dados pessoais ou sensíveis definidos pela Lei de Privacidade Aplicável.

- *Documentação de Segurança* significa as Certificações de Conformidade e os Relatórios SOC.
- *Medidas de Segurança* tem o significado definido na Seção 7.1.1 (Medidas de Segurança do Google).
- *Serviços* refere-se aos serviços aplicáveis descritos no Apêndice 4 (Produtos Específicos).
- *Relatórios SOC* tem o significado atribuído na Seção 7.4 (Certificações de Conformidade e Relatórios SOC).
- *Subprocessador* indica um terceiro autorizado como outro operador nos termos deste Aditivo a tratar os Dados do Parceiro para fornecer partes dos Serviços e SSTs.
- *Autoridade Supervisora* significa, conforme aplicável: (a) uma autoridade supervisora, conforme definição no GDPR da UE; e/ou (b) o Comissário, conforme definição no GDPR do Reino Unido e/ou na FADP da Suíça.
- *FADP da Suíça* refere-se, conforme aplicável, à Lei Federal de Proteção de Dados da Suíça (19 de junho de 1992), juntamente com o Regulamento à Lei Federal de Proteção de Dados (14 de junho de 1993); ou à Lei Federal de Proteção de Dados revisada da Suíça (25 de setembro de 2020), juntamente com o Regulamento à Lei Federal de Proteção de Dados (31 de agosto de 2022).
- *Vigência* significa o período compreendido entre o Início da Vigência do Aditivo e o término da prestação dos Serviços pelo Google, incluindo, se aplicável, qualquer período em que a prestação dos Serviços esteja suspensa e qualquer período após o término em que o Google continue oferecendo os Serviços para fins de transição.
- *GDPR do Reino Unido* refere-se ao GDPR da União Europeia, conforme alterado e incorporado à legislação do Reino Unido pela Lei de Retirada da União Europeia de 2018 e pela legislação secundária aplicável promulgada sob essa lei.

2.2 Os termos "dados pessoais", "titular dos dados", "tratamento", "controlador" e "operador", conforme utilizados neste Aditivo, têm os significados atribuídos pela Lei de Privacidade Aplicável ou, na ausência de tal definição ou lei, pelo GDPR da União Europeia.

2.3 Os termos "titular dos dados", "controlador" e "operador" incluem, respectivamente, "consumidor", "empresa" e "provedor de serviços", conforme exigido pela Lei de Privacidade Aplicável.

3. Duração

Independente de o Contrato ter sido rescindido ou ter expirado, este Aditivo permanecerá em vigor até que, e expirará automaticamente quando, o Google exclua todos os Dados do Parceiro, conforme descrito neste Aditivo.

4. Funções; Conformidade Legal

4.1 *Funções das Partes*. O Google é o operador, e o Parceiro é o controlador ou operador, conforme aplicável, dos Dados Pessoais do Parceiro.

4.2 *Resumo do Tratamento*. O objeto em questão e os detalhes do tratamento dos Dados Pessoais do Parceiro estão descritos no Apêndice 1 (Objeto em Questão e Detalhes do Tratamento de Dados).

4.3 *Conformidade com a Lei*. Cada parte cumprirá com suas obrigações relacionadas ao tratamento dos Dados Pessoais do Parceiro, nos termos da Lei de Privacidade Aplicável.

4.4 *Termos Legais Adicionais*. Na medida em que o tratamento dos Dados Pessoais do Parceiro estiver sujeito a uma Lei de Privacidade Aplicável descrita no Apêndice 3 (Leis de Privacidade Específicas), os termos correspondentes desse apêndice serão aplicados em complemento a estes Termos Gerais e prevalecerão em caso de conflito, conforme descrito na Seção 14.1 (Precedência).

5. Tratamento de Dados

5.1 *Parceiros Operadores*. Se o Parceiro for operador:

a. Ele garante, de forma contínua, que o Cliente e o terceiro controlador autorizaram:

i. As Instruções

ii. O envolvimento do Google pelo Parceiro como outro operador

iii. O envolvimento de Subprocessadores pelo Google, conforme descrito na Seção 11 (Subprocessadores)

b. O Parceiro encaminhará ao Cliente e ao terceiro controlador, de forma imediata e sem demora injustificada, qualquer notificação enviada pelo Google nos termos da Seção 7.2.1 (Notificação de Incidentes), 9.2.1 (Responsabilidade pelas Solicitações) ou 11.4 (Direito de Oposição a Subprocessadores).

c. O Parceiro poderá disponibilizar ao Cliente e ao terceiro controlador outras informações divulgadas pelo Google, nos termos deste Aditivo, sobre as localizações dos Data Centers do Google, além dos nomes, localizações e atividades dos Subprocessadores.

5.2 *Conformidade com as Instruções do Parceiro*. O Parceiro instrui o Google a tratar os Dados do Parceiro segundo os termos do Contrato (inclusive deste Aditivo), apenas da seguinte forma:

a. Para oferecer, proteger e monitorar os Serviços e SSTs

b. Conforme especificado em maiores detalhes:

i. No uso dos Serviços e dos SSTs pelo Parceiro (incluindo via Admin Console)

ii. Em outras instruções escritas fornecidas pelo Parceiro e reconhecidas pelo Google como instruções nos termos deste Aditivo

(coletivamente, as *Instruções*.)

O Google cumprirá as Instruções, salvo se proibido pela Legislação Europeia (quando a Lei Europeia de Proteção de Dados for aplicável) ou pela legislação pertinente (se outra Lei de Privacidade Aplicável estiver em vigor).

6. Exclusão de Dados

6.1 *Exclusão pelo Parceiro*. O Google permitirá que o Parceiro exclua os Dados do Parceiro durante a Vigência, de acordo com a funcionalidade dos Serviços. Se o Parceiro utilizar os Serviços para excluir Dados do Parceiro durante a Vigência e esses dados não puderem ser recuperados pelo Parceiro, tal uso constituirá uma Instrução ao Google para excluir os respectivos Dados do Parceiro dos sistemas do Google. O Google cumprirá essa Instrução assim que razoavelmente possível e dentro do prazo máximo de 180 dias, a menos que a Legislação Europeia exija a retenção (quando aplicável à Lei Europeia de Proteção de Dados) ou se a legislação relevante exigir a retenção (quando outra Lei de Privacidade Aplicável for pertinente).

6.2 *Devolução ou Exclusão ao Término da Vigência*. Se o Parceiro quiser reter Dados do Parceiro após o término da Vigência, poderá instruir o Google, nos termos da Seção 9.1 (Acesso; Retificação; Tratamento Restrito; Portabilidade), a enviar de volta essas informações ainda durante a Vigência. O Parceiro instrui o Google a excluir todos os Dados remanescentes do Parceiro (incluindo cópias) dos sistemas do Google ao Término da Vigência. Após um período de recuperação de até 30 dias a contar dessa data, o Google cumprirá essa Instrução assim que razoavelmente possível e no prazo máximo de 180 dias exceto se a Legislação Europeia exigir a retenção (quando aplicável à Lei Europeia de Proteção de Dados) ou se a legislação relevante exigir a retenção (quando outra Lei de Privacidade Aplicável for pertinente).

7. Segurança de Dados

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

7.1.1 *Medidas de Segurança do Google*. O Google implementará e manterá medidas técnicas, organizacionais e físicas para proteger os Dados do Parceiro contra destruição, perda, alteração, divulgação ou acesso ilícitos ou acidentais, conforme descrito no Apêndice 2 (Medidas de Segurança), as *Medidas de Segurança*. Elas incluem meios de criptografar os Dados do Parceiro para ajudar a garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços do Google; para auxiliar na restauração do acesso rápido aos Dados do Parceiro após um incidente; e para fazer testes regulares de eficácia. O Google poderá atualizar as Medidas de Segurança periodicamente, desde que essas atualizações não resultem em uma redução concreta da segurança dos Serviços.

7.1.2 *Acesso e Conformidade*. O Google:

a. Autorizará os funcionários, contratados e Subprocessadores do Google a acessar os Dados do Parceiro apenas quando estritamente necessário para cumprir as Instruções.

b. Tomará as providências adequadas para garantir o cumprimento das Medidas de Segurança pelos empregados, contratados e Subprocessadores do Google, na medida em que forem aplicáveis ao âmbito de atuação.

c. Garantirá que todas as pessoas autorizadas a tratar os Dados do Parceiro estejam sujeitas a uma obrigação de confidencialidade.

7.1.3 *Controles de Segurança Adicional.* O Google disponibilizará de Controles de Segurança Adicionais para:

a. Permitir que o Parceiro tome medidas para proteger os Dados do Parceiro.

b. Fornecer ao Parceiro informações sobre segurança, acesso e uso dos Dados do Parceiro.

7.1.4 *Assistência de Segurança do Google.* O Google, considerando a natureza do tratamento dos Dados Pessoais do Parceiro e as informações disponíveis ao Google, ajudará o Parceiro no cumprimento das próprias obrigações (ou, quando o Parceiro for operador, das obrigações do terceiro controlador) relacionadas à segurança e às violações de dados pessoais, nos termos da Lei de Privacidade Aplicável. Para isso, o Google:

a. Implementará as Medidas de Segurança e garantirá a manutenção delas, de acordo com a Seção 7.1.1 (Medidas de Segurança do Google).

b. Disponibilizará Controles de Segurança Adicionais, conforme estabelecido na Seção 7.1.3 (Controles de Segurança Adicionais).

c. Cumprirá os termos da Seção 7.2 (Incidentes de Dados).

d. Disponibilizará a Documentação de Segurança, conforme estabelecido na Seção 7.5.1 (Revisões da Documentação de Segurança) e fornecerá as informações contidas no Contrato (inclusive neste Aditivo).

e. Cooperará e fornecerá outras formas razoáveis de assistência, mediante solicitação do Parceiro, se as subseções (a) a (d) acima forem insuficientes para que o Parceiro (ou o terceiro controlador) cumpra tais obrigações.

7.2 *Incidentes de Dados.*

7.2.1 *Notificação de Incidentes.* O Google notificará o Parceiro de forma imediata e sem demora injustificada após tomar conhecimento de um Incidente de Dados, além de tomar prontamente as medidas razoáveis para minimizar danos e proteger os Dados do Parceiro.

7.2.2 *Detalhes do Incidente de Dados.* A notificação do Google sobre um Incidente de Dados descreverá: a natureza do Incidente de Dados, incluindo os recursos do Parceiro que foram afetados; as medidas que o Google tomou ou planeja tomar para tratar o Incidente de Dados e mitigar os possíveis riscos; as medidas que o Google recomendar ao Parceiro para lidar com o Incidente de Dados; e os detalhes de um ponto de contato para conseguir 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 demoras injustificadas assim que estiverem disponíveis.

7.2.3 *Nenhuma Avaliação de Dados do Parceiro Feita pelo Google.* O Google não tem a obrigação de avaliar os Dados do Parceiro para identificar informações sujeitas a exigências legais específicas.

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

7.3 *Responsabilidades e Avaliação de Segurança do Parceiro*.

7.3.1 *Responsabilidades de Segurança do Parceiro*. Sem prejuízo das obrigações do Google previstas nas Seções 7.1 (Medidas, Controles e Assistência de Segurança do Google) e 7.2 (Incidentes de Dados), e em outras disposições do Contrato, entre Google e Parceiro, o Parceiro é responsável pelo uso dos Serviços por si e pelos Clientes dele, bem como pelo armazenamento de cópias dos Dados do Parceiro fora dos sistemas do Google ou dos Subprocessadores do Google, incluindo:

a. Utilizar os Serviços e os Controles de Segurança Adicionais para garantir um nível de segurança apropriado ao risco referente aos Dados do Parceiro.

b. Proteger as credenciais de autenticação de contas, os sistemas e os dispositivos que o Parceiro e os Clientes dele utilizam para acessar os Serviços.

c. Realizar o backup dos Dados do Parceiro, conforme apropriado.

7.3.2 *Avaliação de Segurança do Parceiro*. O Parceiro concorda que os Serviços, as Medidas de Segurança, os Controles de Segurança Adicionais e os compromissos assumidos pelo Google nos termos da Seção 7 (Segurança de Dados) proporcionam um nível de segurança adequado aos riscos associados aos Dados do Parceiro (considerando o estado da técnica, os custos de implementação, a natureza, o escopo, o contexto e as finalidades do tratamento dos Dados do Parceiro, bem como os riscos para os titulares dos dados).

7.4 *Certificações de Conformidade e Relatórios SOC*. O Google manterá, para os Serviços Auditados, pelo menos os seguintes itens para verificar a efetividade contínua das Medidas de Segurança:

a. Certificados ISO 27001 e outras certificações descritas no Apêndice 4 (Produtos Específicos), as *Certificações de Conformidade*.

b. Relatórios SOC 2 e SOC 3 produzidos pelo Auditor Independente do Google e atualizados anualmente com base em auditoria realizada pelo menos uma vez a cada 12 (doze) meses (*Relatórios SOC*).

O Google poderá adicionar padrões a qualquer momento. O Google poderá substituir uma Certificação de Conformidade ou Relatório SOC por uma alternativa equivalente ou aprimorada.

7.5 *Revisões e Auditorias de Conformidade*.

7.5.1 *Revisões da Documentação de Segurança*. Para demonstrar a conformidade do Google com as obrigações nos termos deste Aditivo, o Google disponibilizará a Documentação de Segurança para o Parceiro revisar e, caso o Parceiro seja operador, o Google permitirá que o Parceiro solicite acesso aos Relatórios SOC para o Cliente e o terceiro controlador, de acordo com a Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

7.5.2 *Direitos de Auditoria do Cliente*.

a. *Auditoria do Parceiro*. O Google permitirá, caso seja exigido pela Lei de Privacidade Aplicável, que o Parceiro ou um auditor independente nomeado por ele realize auditorias (incluindo inspeções) para verificar o cumprimento, pelo Google, das obrigações dele previstas neste Aditivo, de acordo com a Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias). Durante uma auditoria, o Google cooperará de forma razoável com o Parceiro ou o auditor dele, conforme descrito na Seção 7.5 (Revisões e Auditorias de Conformidade).

b. *Revisão Independente do Parceiro*. O Parceiro poderá realizar uma auditoria para verificar o cumprimento, pelo Google, das obrigações dele previstas neste Aditivo, revisando a Documentação de Segurança (que reflete o resultado das auditorias conduzidas pelo Auditor Terceirizado do Google).

7.5.3 *Termos Comerciais Adicionais para Revisões e Auditorias*.

a. O Parceiro deverá entrar em contato com a Equipe de Proteção de Dados da Nuvem do Google para pedir:

i. Acesso aos Relatórios SOC para um terceiro controlador, nos termos da Seção 7.5.1 (Revisões da Documentação de Segurança).

ii. Uma auditoria, conforme os termos da Seção 7.5.2 (a. Auditoria do Parceiro).

b. Após um pedido do Parceiro nos termos da Seção 7.5.3 (a), o Google e o Parceiro deverão discutir e concordar previamente sobre:

i. Os controles de segurança e confidencialidade aplicáveis a qualquer acesso aos Relatórios SOC por um terceiro controlador, nos termos da Seção 7.5.1 (Revisões da Documentação de Segurança).

ii. A data de início, o escopo e a duração razoáveis, bem como os controles de segurança e confidencialidade aplicáveis a qualquer auditoria nos termos da Seção 7.5.2 (a. Auditoria do Parceiro).

c. O Google poderá cobrar uma taxa (com base em custos razoáveis) por qualquer auditoria realizada nos termos da Seção 7.5.2 (a. Auditoria do Parceiro). O Google enviará ao Parceiro mais detalhes sobre qualquer taxa aplicável e sobre a base de cálculo antes de auditorias desse tipo. O Parceiro será responsável pelas taxas cobradas por um auditor terceirizado indicado por ele para executar a auditoria.

d. O Google poderá se opor, por escrito, a um auditor nomeado pelo Parceiro para realizar qualquer auditoria nos termos da Seção 7.5.2 (a. Auditoria do Parceiro), caso o auditor, na opinião razoável do Google, não seja devidamente qualificado ou independente, seja concorrente do Google ou, de outra forma, manifestamente inadequado. Qualquer objeção feita pelo Google exigirá que o Parceiro indique outro auditor ou conduza a auditoria por conta própria.

e. Quaisquer solicitações do Parceiro nos termos do Apêndice 3 (Leis de Privacidade Específicas) ou do Apêndice 4 (Produtos Específicos) referentes ao acesso a Relatórios SOC de um terceiro

controlador ou à realização de auditorias também estarão sujeitas à Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

8. Revisões de Impacto e Consultas

O Google, considerando a natureza do tratamento e as informações disponíveis ao Google, auxiliará o Parceiro no cumprimento das obrigações dele (ou, quando o Parceiro for o operador, das obrigações do terceiro controlador) relativas a avaliações de proteção de dados, avaliações de risco, consultas prévias a autoridades regulatórias ou procedimentos equivalentes, nos termos da Lei de Privacidade Aplicável, ao:

a. Disponibilizar os Controles de Segurança Adicionais em conformidade com a Seção 7.1.3 (Controles de Segurança Adicionais) e a Documentação de Segurança nos termos da Seção 7.5.1 (Revisões da Documentação de Segurança).

b. Enviar as informações contidas no Contrato (inclusive neste Aditivo).

c. Se as subseções (a) e (b) acima forem insuficientes para que o Parceiro (ou o terceiro controlador) cumpra tais obrigações, o Google, mediante pedido do Parceiro, cooperará e prestará a assistência razoável necessária.

9. Acesso etc.; Direitos do Titular dos Dados; Exportação de Dados

9.1 *Acesso, Retificação, Tratamento Restrito e Portabilidade*. Durante a Vigência, o Google permitirá que o Parceiro, de acordo com a funcionalidade dos Serviços, acesse, retifique e restrinja o tratamento dos Dados do Parceiro, inclusive pela funcionalidade de exclusão fornecida pelo Google, conforme descrito na Seção 6.1 (Exclusão pelo Parceiro), além de exportar os Dados do Parceiro. Se o Parceiro tomar conhecimento de que Dados Pessoais do Parceiro estão imprecisos ou desatualizados, será de responsabilidade dele usar essa função para retificar ou excluir os dados, caso exigido pela Lei de Privacidade Aplicável.

9.2 *Solicitações dos Titulares dos Dados*.

9.2.1 *Responsabilidade pelas Solicitações*. Durante a Vigência, caso a Equipe de Proteção de Dados da Nuvem do Google receba um pedido de um titular de dados relacionado a Dados Pessoais do Parceiro e que identifique o Parceiro, o Google:

a. Orientará o titular de dados a encaminhar a solicitação ao Parceiro.

b. Notificará o Parceiro prontamente.

c. Não responderá à solicitação do titular de dados sem autorização do Parceiro.

O Parceiro deverá responder a qualquer uma dessas solicitações, inclusive, quando necessário, utilizando a funcionalidade dos Serviços.

9.2.2 *Assistência a Solicitações de Titulares de Dados do Google*. O Google, considerando a natureza do tratamento dos Dados Pessoais do Parceiro, auxiliará o Parceiro no cumprimento das obrigações

dele (ou, quando o Parceiro for o operador, das obrigações do terceiro controlador) previstas na Lei de Privacidade Aplicável para responder a solicitações de exercício de direitos dos titulares de dados, ao:

a. Disponibilizar Controles de Segurança Adicionais, conforme estabelecido na Seção 7.1.3 (Controles de Segurança Adicionais).

b. Cumprir as Seções 9.1 (Acesso; Retificação; Tratamento Restrito; Portabilidade) e 9.2.1 (Responsabilidade pelas Solicitações).

c. Se as subseções (a) e (b) acima forem insuficientes para que o Parceiro (ou o terceiro controlador) cumpra tais obrigações, o Google, mediante pedido do Parceiro, cooperará e prestará a assistência razoável necessária.

10. Locais de Tratamento de Dados

10.1 *Instalações de Armazenamento e Tratamento de Dados*. Observadas as obrigações do Google quanto à localização de dados previstas nos Termos Específicos do Serviço e quanto à transferência de dados constantes do Apêndice 3 (Leis de Privacidade Específicas), se aplicável, os Dados do Parceiro poderão ser tratados em qualquer país onde o Google ou os Subprocessadores dele mantêm instalações.

10.2 *Informações do Data Center*. Os locais dos data centers do Google estão descritos no Apêndice 4 (Produtos Específicos).

11. Subprocessadores

11.1 *Consentimento para o Envolvimento de Subprocessadores*. O Parceiro autoriza expressamente o Google a contratar como Subprocessadores as entidades divulgadas conforme descrito na Seção 11.2 (Informações sobre Subprocessadores), no Início da Vigência deste Aditivo. Além disso, sem prejuízo da Seção 11.4 (Direito de Oposição a Subprocessadores), o Parceiro autoriza, de forma geral, o Google a contratar terceiros como Subprocessadores (*Novos Subprocessadores*).

11.2 *Informações sobre Subprocessadores*. Os nomes, locais e atividades dos Subprocessadores são descritos no Apêndice 4 (Produtos Específicos).

11.3 *Requisitos para a Contratação de Subprocessadores*. Ao contratar qualquer Subprocessador, o Google deverá:

a. Garantir, em um contrato por escrito, que:

i. O Subprocessador somente acessará e utilizará os Dados do Parceiro na medida necessária para o cumprimento das obrigações a ele subcontratadas, e o fará em conformidade com o Contrato (inclusive este Aditivo).

ii. Se exigido pelas Leis de Privacidade Aplicáveis, as obrigações de proteção de dados descritas neste Aditivo serão impostas ao Subprocessador, conforme detalhado no Apêndice 3 (Leis de Privacidade Específicas).

b. Permanecer totalmente responsável por todas as obrigações subcontratadas e por todos os atos e omissões por parte do Subprocessador.

11.4 *Direito de Oposição a Subprocessadores*.

a. Quando o Google contratar qualquer Novo Subprocessador durante a Vigência, notificará o Parceiro da contratação (incluindo o nome, a localidade e as atividades do Novo Subprocessador) com, no mínimo, 30 dias antes do início do tratamento de quaisquer Dados do Parceiro pelo Novo Subprocessador.

b. O Parceiro poderá, no prazo de 90 dias após ser notificado da contratação de um Novo Subprocessador, manifestar sua oposição mediante a rescisão imediata do Contrato por conveniência:

i. Nos termos da previsão de rescisão imotivada constante do Contrato.

ii. Caso não exista tal previsão, notifique o Google.

12. Equipe de Proteção de Dados do Cloud; Tratamento de Registros

12.1 *Equipe de Proteção de Dados do Cloud*. A Equipe de Proteção de Dados do Cloud do Google prestará apoio célere e razoável a quaisquer questionamentos do Parceiro relacionados ao tratamento dos Dados do Parceiro, nos termos do Contrato, podendo ser consultada conforme previsto na cláusula de Notificações do Contrato ou no Apêndice 4 (Produtos Específicos).

12.2 *Registros de Tratamento do Google*. O Google manterá a documentação adequada das atividades de tratamento dele, conforme exigido pela Lei de Privacidade Aplicável. Na medida em que qualquer Lei de Privacidade Aplicável exigir que o Google colete e mantenha registros de determinadas informações relativas ao Parceiro ou a seus Clientes, caberá ao Parceiro utilizar o Admin Console ou demais meios indicados no Apêndice 4 (Produtos Específicos) para fornecer tais informações, mantendo-as corretas e atualizadas. O Google poderá disponibilizar tais informações às autoridades competentes, incluindo uma Autoridade de Controle, caso seja exigido pela Lei de Privacidade Aplicável.

12.3 *Solicitações de Controladores*. Durante a Vigência, caso a Equipe de Proteção de Dados do Cloud do Google receba uma solicitação ou instrução de um terceiro que se apresente como controlador dos Dados Pessoais do Parceiro, o Google orientará esse terceiro a entrar em contato com o Parceiro.

13. Notificações

As notificações previstas neste Aditivo (incluindo comunicações sobre quaisquer Incidentes de Dados) serão encaminhadas ao Endereço de E-mail de Notificação. Caberá ao Parceiro utilizar o Admin Console, ou outro meio de comunicação para notificar o Google e garantir que seu Endereço de E-mail de Notificação permaneça atualizado e válido.

14. Interpretação

14.1 *Precedência*. Em caso de conflito entre:

a. O Apêndice 3 (Leis de Privacidade Específicas) e o restante do Aditivo, incluindo o Apêndice 4 (Produtos Específicos), prevalecerá o Apêndice 3.

b. O Apêndice 4 (Produtos Específicos) e o restante do Aditivo, com exceção do Apêndice 3, prevalecerá o Apêndice 4.

c. Este Aditivo e o restante do Contrato, prevalecerá este Aditivo.

14.2 *Referências da Seção*. Salvo indicado de outra forma, as referências a seções de qualquer Apêndice deste Aditivo referem-se às seções dos Termos Gerais do próprio Aditivo.

14.3 *Clientes*. Para evitar dúvidas, os Clientes não são terceiros beneficiários deste Aditivo.

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

Objeto em Questão

A prestação dos Serviços e do Suporte Técnico ao Parceiro pelo Google.

Duração do Tratamento

A Vigência somada ao período do término dela até a exclusão de todos os Dados do Parceiro pelo Google, em conformidade com este Aditivo.

Natureza e Finalidade do Tratamento

O Google tratará os Dados Pessoais do Parceiro com a finalidade de prestar os Serviços e os SSTs ao Parceiro, em conformidade com este Aditivo.

Categorias de Dados

Dados referentes a pessoas físicas fornecidos ao Google por meio dos Serviços pelo Parceiro, os Clientes dele ou os Usuários Finais do Parceiro, ou sob orientação destes.

Titulares dos dados

Os titulares de dados são as pessoas físicas cujos dados são fornecidos ao Google por meio dos Serviços, seja pelo Parceiro, por seus Clientes, por Usuários Finais do Parceiro ou sob orientação de qualquer uma dessas partes.

Apêndice 2: Medidas de Segurança

A partir do Início da Vigência deste Aditivo, o Google implementará e manterá as Medidas de Segurança descritas neste Apêndice 2.

1. Segurança de Redes e Data Centers

(a) Data centers

Infraestrutura. O Google opera data centers em várias regiões do mundo. O Google armazena todos os dados de produção em data centers fisicamente seguros.

Redundância. Os sistemas de infraestrutura foram projetados para eliminar pontos únicos de falha e minimizar o impacto dos riscos ambientais previstos. Circuitos duplos, interruptores, redes ou outros dispositivos necessários ajudam a proporcionar essa redundância. Os Serviços foram criados para permitir que o Google execute certos tipos de manutenção preventiva e corretiva sem interrupções. Todos os equipamentos e instalações ambientais possuem procedimentos documentados de manutenção preventiva, os quais detalham o processo e a periodicidade das atividades, conforme as especificações internas ou do fabricante. A manutenção preventiva e corretiva dos equipamentos do data center é realizada conforme programação estabelecida em processo de mudança padrão, seguindo os procedimentos documentados.

Eletricidade. Os sistemas de energia elétrica dos data centers são projetados para oferecer redundância e facilidade de manutenção, garantindo que não haja impacto nas operações contínuas, que funcionam 24 horas por dia, 7 dias por semana. Na maioria dos casos, os componentes de infraestrutura crítica do data center contam com uma fonte principal de energia e uma fonte alternativa, ambas com capacidade equivalente. A energia de reserva é garantida por diversos mecanismos, como baterias de no-breaks (UPS), que oferecem proteção de energia de forma consistente e confiável durante quedas de energia, apagões, sobretensões, subtensões e variações de frequência fora dos parâmetros tolerados. Em caso de interrupção no fornecimento de energia, a alimentação de reserva garante eletricidade ao data center na capacidade total por até 10 minutos, até a ativação dos geradores de backup. Os geradores de reserva podem ser acionados automaticamente em poucos segundos, fornecendo energia elétrica emergencial suficiente para manter o data center na capacidade total, normalmente por vários dias.

Sistemas Operacionais do Servidor. Os servidores do Google usam uma implementação baseada em Linux personalizada para o ambiente do aplicativo. Os dados são armazenados usando algoritmos proprietários para aumentar a segurança e redundância desses dados.

Qualidade do Código. O Google emprega um processo de revisão de código para aumentar a segurança do código usado para prestar os Serviços e aprimorar os produtos de segurança em ambientes de produção.

Continuidade de Negócios. O Google desenvolve, planeja e testa regularmente programas de recuperação de desastres e de continuidade dos negócios.

(b) Redes e Transmissão.

Transmissão de Dados. Os data centers são, em geral, conectados por links privados de alta velocidade, proporcionando transferência de dados rápida e segura entre as unidades. Essa configuração é projetada para impedir que os dados sejam lidos, copiados, alterados ou removidos sem autorização durante a transferência eletrônica, o transporte ou o processo de gravação em mídias de armazenamento. O Google transfere dados por protocolos padrão da Internet.

Superfície de Ataque Externa. O Google emprega várias camadas de dispositivos de rede e detecção de invasões para proteger sua superfície de ataque externa. São considerados os possíveis vetores de

ataque e incorporadas tecnologias específicas adequadas à proteção de sistemas expostos externamente.

Detecção de Intrusões. A detecção de intrusões fornece informações sobre atividades de ataque em andamento, bem como dados relevantes para a resposta a incidentes. A detecção de intrusões do Google envolve um rigoroso controle do tamanho e da composição da superfície de ataque, utilizando medidas preventivas aliadas a controles inteligentes de detecção nos pontos de entrada de dados, além da adoção de tecnologias capazes de mitigar automaticamente situações de risco.

Resposta a Incidentes. O Google monitora diversos canais de comunicação para identificar incidentes de segurança, e sua equipe de segurança atua prontamente na resposta a incidentes detectados.

Tecnologias de Criptografia. O Google disponibiliza criptografia HTTPS (também chamada de conexão SSL ou TLS). Os servidores do Google oferecem suporte à troca de chaves criptográficas Diffie-Hellman por meio de curvas elípticas efêmeras, assinadas com RSA e ECDSA. Esses métodos de perfect forward secrecy (PFS) contribuem para proteger o tráfego e minimizam o impacto em caso de comprometimento de uma chave ou de avanços em criptografia.

2. Controles de Acesso e Local

(a) Controles do Local.

Operação de segurança no data center local. Os data centers do Google contam com operações de segurança presencial responsáveis por todas as funções de segurança física do local, 24 horas por dia, 7 dias por semana. A equipe responsável pela segurança local monitora as câmeras de circuito fechado de TV (CCTV) e todos os sistemas de alarme. Essa equipe realiza patrulhas internas e externas no data center regularmente.

Procedimentos de Acesso ao Data Center. O Google adota procedimentos formais para autorização de acesso físico aos data centers. Os data centers estão localizados em instalações que requerem acesso por cartão eletrônico, com alarmes conectados à equipe de segurança no local. Todos os visitantes e profissionais que acessam o data center devem se identificar e apresentar um documento de identificação à equipe de operações de segurança no local. Somente funcionários, contratados e visitantes devidamente autorizados podem ingressar nos data centers. Somente funcionários e contratados devidamente autorizados podem solicitar o acesso por meio de chave eletrônica a essas instalações. As solicitações de acesso por cartão eletrônico ao data center devem ser realizadas por e-mail e requerem a aprovação do gerente do solicitante e do diretor do data center. Todos os demais indivíduos que necessitem de acesso temporário ao data center devem: (i) obter aprovação prévia dos gerentes responsáveis pelo data center específico e pelas áreas internas a serem visitadas; (ii) realizar o registro de entrada junto à equipe de operações de segurança local; e (iii) apresentar um registro de acesso ao data center devidamente aprovado, que identifique o indivíduo como autorizado.

Dispositivos de Segurança do Data Center Local. Os data centers do Google utilizam um sistema de controle de acesso com autenticação dupla, vinculado a um sistema de alarme. O sistema de controle de acesso monitora e registra o uso da chave eletrônica de cada indivíduo, bem como o momento em que acessa as portas de perímetro, a área de recebimento e envio e outras áreas críticas. Atividades não autorizadas e tentativas de acesso mal-sucedidas são registradas pelo sistema de controle de

acesso e investigadas, quando aplicável. O acesso autorizado em todas as operações comerciais e data centers é restrito conforme as zonas estabelecidas e as responsabilidades de trabalho de cada indivíduo. As portas corta-fogo dos data centers são equipadas com alarmes. As câmeras de circuito fechado de TV (CCTV) operam continuamente nas áreas internas e externas dos data centers. O posicionamento das câmeras foi planejado para abranger áreas estratégicas, incluindo, entre outras, o perímetro, os acessos ao edifício do data center e as áreas de envio e recebimento. A equipe de operações de segurança local é responsável pela gestão dos equipamentos de monitoramento, gravação e controle do sistema de CFTV. Todos os data centers possuem cabeamento protegido para conectar os equipamentos de CFTV. As câmeras realizam gravações contínuas do local, por meio de sistemas digitais, 24 horas por dia, 7 dias por semana. Os registros de vigilância são mantidos por até 30 dias com base na atividade.

(b) Controle de Acesso.

Equipe de Segurança da Infraestrutura. O Google possui e mantém uma política de segurança aplicável ao seu quadro de pessoal, exigindo a participação em treinamentos de segurança como parte do programa de capacitação da equipe. A equipe de segurança de infraestrutura do Google é responsável pelo monitoramento contínuo dessa infraestrutura, pela análise dos Serviços e pela resposta a incidentes de segurança.

Gerenciamento de Privilégios e Controle de Acesso. Os Administradores do Parceiro e os Usuários Finais do Parceiro devem se autenticar por meio de um sistema central de autenticação ou de um sistema de logon único para utilizar os Serviços.

Políticas e Processos Internos de Acesso a Dados — Política de Acesso. Os processos e políticas de acesso a dados internos do Google são projetados para evitar que pessoas e sistemas não autorizados consigam acesso a sistemas usados para tratar Dados Pessoais. O Google projeta seus sistemas para (i) permitir que as pessoas autorizadas acessem apenas os dados que estão autorizadas a acessar; e (ii) garantir que os Dados Pessoais não possam ser lidos, copiados, alterados ou removidos sem autorização durante o tratamento, uso e após a gravação. Os sistemas são desenvolvidos para detectar qualquer acesso inadequado. O Google emprega um sistema de gerenciamento de acesso centralizado para controlar o acesso de pessoal aos servidores de produção e fornece acesso apenas a um número limitado de funcionários autorizados. Os sistemas de autenticação e autorização do Google utilizam certificados SSH e chaves de segurança, sendo projetados para fornecer à empresa mecanismos de acesso seguros e flexíveis. Esses mecanismos são projetados para conceder somente direitos de acesso aprovado a hosts, registros, dados e informações de configuração do site. O Google exige o uso de códigos de usuário exclusivos, senhas fortes, autenticação de dois fatores e listas de acesso cuidadosamente monitoradas para minimizar o potencial de uso não autorizado da conta. A concessão ou modificação de direitos de acesso é baseada em: responsabilidades do trabalho do pessoal autorizado, deveres de trabalho necessários para executar tarefas autorizadas e com base em uma necessidade de saber. A concessão ou modificação de direitos de acesso também precisa estar 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 pelo menos as práticas padrão do

setor. Esses padrões incluem restrições sobre reutilização e nível de segurança das senhas. Para acesso a informações extremamente sensíveis (por exemplo, dados de cartão de crédito), o Google usa tokens de hardware.

3. Dados

(a) *Armazenamento, Isolamento e Registro de Dados.* O Google armazena dados em ambiente multilocatário, em servidores de sua propriedade. Observadas eventuais Instruções em sentido contrário (por exemplo, quanto à seleção da localização dos dados), o Google replica os Dados do Parceiro entre diversos data centers em várias regiões. O Google também isola logicamente os Dados do Parceiro. O Parceiro receberá o controle de políticas específicas de compartilhamento de dados pessoais. Essas políticas, em conformidade com a funcionalidade dos Serviços, permitirão ao Parceiro determinar as configurações de compartilhamento de produtos aplicáveis aos Usuários Finais do Parceiro para finalidades específicas. O Parceiro pode optar por utilizar a geração de registros disponibilizada pelo Google por meio dos Serviços.

(b) *Discos Desativados e Política de Limpeza de Discos*. Alguns discos que armazenam dados podem apresentar problemas de desempenho, erros ou falhas de hardware, o que pode resultar em sua desativação ("Disco Desativado"). Todos os Discos Desativados passam por uma série de processos de destruição de dados ("Política de Limpeza de Discos") antes de serem retirados das instalações do Google para reutilização ou descarte. Os Discos Desativados são apagados em um processo de várias etapas e verificados por pelo menos dois validadores 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 monitorar a conformidade com a Política de Limpeza de Discos.

4. Segurança de Pessoal

A equipe do Google deve agir em conformidade com as diretrizes da empresa relativas à 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 estatutárias aplicáveis.

A equipe precisa assinar um acordo de confidencialidade e confirmar o recebimento das Políticas de Privacidade e confidencialidade do Google e a conformidade com elas. A equipe recebe treinamento de segurança. Os profissionais que lidam com os Dados do Parceiro devem cumprir requisitos adicionais adequados às suas funções, como, por exemplo, a obtenção de certificações. O pessoal do Google não tratará os Dados do Parceiro sem autorização.

5. Segurança do Subprocessador

Antes da integração, o Google realiza auditorias das práticas de segurança e privacidade dos Subprocessadores para garantir que eles forneçam um nível de proteção adequado em relação ao acesso aos dados e ao escopo dos serviços a serem prestados. Após a avaliação do Google dos riscos apresentados pelo Subprocessador, e observados os requisitos descritos na Seção 11.3 (Requisitos

para Contratação de Subprocessadores), o Subprocessador deverá firmar termos contratuais adequados quanto à segurança, confidencialidade e privacidade.

Apêndice 3 (Leis de Privacidade Específicas)

Os termos de cada subseção deste Apêndice 3 aplicam-se somente quando a respectiva legislação for aplicável ao tratamento dos Dados Pessoais do Parceiro.

Legislação Europeia de Proteção de Dados

1. Definições Adicionais.

- *País Adequado* refere-se a:

(a) Dados tratados sujeitos ao GDPR da União Europeia: o Espaço Econômico Europeu ou um país ou território com proteção considerada adequada nos termos do GDPR da UE.

(b) Dados tratados sujeitos ao GDPR do Reino Unido: o Reino Unido ou qualquer país ou território com proteção de dados considerada adequada pelo GDPR do Reino Unido e pela Lei Geralde Proteção de Dados de 2018.

(c) Dados tratados sujeitos à FADP da Suíça: a Suíça, ou qualquer país ou território que: (i) esteja incluído na lista de Estados cuja legislação assegura proteção adequada, conforme publicada pelo Comissário Federal de Proteção de Dados e Informação da Suíça, se aplicável; ou (ii) seja reconhecido pelo Conselho Federal Suíço como assegurando proteção adequada nos termos da FADP da Suíça.

Em todos os casos, exceto quando a referência é um regime opcional de proteção de dados.

- *"Solução Alternativa de Transferência* significa", para o propósito dos termos da Lei Geral de Proteção de Dados, uma solução, diferente das SCCs, que permite a transferência legal de dados pessoais para um terceiro país, em conformidade com a Legislação Europeia de Proteção de Dados, por exemplo, um regime de proteção de dados reconhecido por assegurar que as entidades participantes ofereçam proteção adequada.

- *"SCCs do Parceiro"* refere-se aos SCCs (Controlador para Processador), as SCCs (Processador para Processador) ou as SCCs (Processador para Controlador), conforme aplicável.

- *"SCCs"* refere-se às Cláusulas Contratuais Padrão do Parceiro ou as SCCs (Processador para Processador, Exportador do Google), conforme aplicável.

- *'SCCs (Controlador para Processador)"* refere-se aos termos disponíveis em: https://cloud.google.com/terms/sccs/eu-c2p

- *"SCCs (Controlador para Controlador)"* refere-se aos termos disponíveis em: https://cloud.google.com/terms/sccs/eu-p2c

- *"SCCs (Processador para Processador)"* refere-se aos termos disponíveis em: https://cloud.google.com/terms/sccs/eu-p2p

- *"SCCs (Processador para Processador, Exportador do Google)"* refere-se aos termos em: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter

2. Notificações de Instrução. Sem prejuízo das obrigações do Google previstas na Cláusula 5.2 (Cumprimento das Instruções do Parceiro) ou de quaisquer outros direitos ou obrigações de qualquer das partes previstas no Contrato, o Google compromete-se a notificar imediatamente o Parceiro caso, a seu juízo:

a. A legislação europeia impeça o Google de cumprir uma Instrução.

b. Uma Instrução não esteja em conformidade com a Legislação Europeia de Proteção de Dados.

c. Caso o Google, por qualquer outro motivo, não possa cumprir uma Instrução, em todos os casos exceto se tal notificação for vedada pela legislação europeia.

Caso o Parceiro atue como operador, deverá encaminhar imediatamente ao terceiro controlador qualquer notificação fornecida pelo Google nos termos desta seção.

3. Direitos de Auditoria do Parceiro. O Google permitirá que o Parceiro, ou auditor independente por ele indicado, realize auditorias (incluindo inspeções) conforme descrito na Seção 7.5.2 (a. Auditoria do Parceiro). Durante a auditoria, o Google disponibilizará todas as informações necessárias para demonstrar o cumprimento das obrigações dele de acordo com este Aditivo e contribuirá para a auditoria conforme descrito nesta e na Seção 7.5 (Revisões e Auditorias de Conformidade).

4. Transferências de Dados.

4.1 *Transferências Restritas.* As partes reconhecem que a Legislação Europeia de Proteção de Dados não exige SCCs ou uma Solução Alternativa de Transferência para que os Dados Pessoais do Parceiro sejam tratados ou transferidos para um País Adequado. Se os Dados Pessoais do Parceiro forem transferidos para qualquer outro país e a Legislação Europeia de Proteção de Dados for aplicável a essas transferências, conforme certificado pelo Parceiro nos termos da Seção 4.2 (Certificação por Parceiros fora da EMEA) destes termos relativos à Legislação Europeia de Proteção de Dados, caso seu endereço de cobrança esteja fora da EMEA, (*Transferências Restritas*), então:

a. Se o Google tiver adotado uma Solução Alternativa de Transferência para quaisquer Transferências Restritas, informará o Parceiro sobre a solução relevante e garantirá que tais Transferências Restritas sejam realizadas em conformidade com essa solução.

b. Se o Google não tiver adotado uma Solução Alternativa de Transferência para quaisquer Transferências Restritas, ou informar ao Parceiro que deixou de adotar tal solução para quaisquer Transferências Restritas (sem adotar uma Solução Alternativa de Substituição).

i. Se o endereço do Google estiver em um País Adequado:

(A) As Cláusulas Contratuais Padrão, SCCs (Processador para Processador da UE, Exportador do Google) serão aplicáveis em relação a todas as Transferências Restritas do Google para Subprocessadores.

b. Além disso, caso o endereço de cobrança do Parceiro não esteja em um País Adequado, as Cláusulas Contratuais Padrão (Processador para Controlador) serão aplicáveis (independentemente de o Parceiro atuar como controlador ou operador) em relação a tais Transferências Restritas entre o Google e o Parceiro.

ii. Caso o endereço do Google não esteja em um País Adequado, as Cláusulas Contratuais Padrão (Controlador para Operador) ou as Cláusulas Contratuais Padrão (Operador para Operador) serão aplicáveis (conforme o Parceiro atue como controlador ou operador) em relação a tais Transferências Restritas entre o Google e o Parceiro.

4.2 *Certificação por Parceiros fora da EMEA.*. Se o endereço de cobrança do Parceiro estiver fora da EMEA e o tratamento dos Dados Pessoais do Parceiro estiver sujeito à Legislação Europeia de Proteção de Dados, então, salvo indicação em contrário no Apêndice 4 (Produtos Específicos) deste Aditivo, o Parceiro deverá certificar tal condição e identificar sua Autoridade Supervisora competente por meio do Admin Console dos Serviços aplicáveis.

4.3 *Informações sobre Transferências Restritas.* O Google fornecerá ao Parceiro informações relevantes sobre Transferências Restritas, Controles de Segurança Adicionais e outras medidas de proteção suplementares:

a. Conforme descrito na Seção 7.5.1 (Revisões da Documentação de Segurança).

b. Em quaisquer outros locais descritos no Apêndice 4 (Produtos Específicos).

c. Em relação à adoção, pelo Google, de uma Solução Alternativa de Transferência, em https://cloud.google.com/terms/alternative-transfer-solution.

4.4 *Auditorias de SCCs.* Se as Cláusulas Contratuais Padrão do Parceiro forem aplicáveis, conforme descrito na Seção 4.1 (Transferências Restritas) destes termos relativos à Legislação Europeia de Proteção de Dados, o Google permitirá que o Parceiro (ou um auditor independente por ele designado) faça auditorias conforme previsto nessas SCCs e, durante a auditoria, todas as informações exigidas por essas Cláusulas, de acordo com a Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

4.5 *SCCs e o terceiro controlador.* Se o Parceiro for um operador, o Parceiro reconhece que o Google, como outro controlador, pode não ser capaz de identificar o terceiro controlador e, consequentemente, o Parceiro encaminhará ao terceiro controlador, de forma imediata e sem atraso injustificado, qualquer notificação que se refira a SCCs.

4.6 *Rescisão em Razão de Risco na Transferência de Dados.* Se o Parceiro concluir, com base em seu uso atual ou pretendido dos Serviços, que não estão sendo fornecidas salvaguardas adequadas para os Dados Pessoais do Parceiro transferidos, o Parceiro poderá rescindir imediatamente o Contrato, de acordo com a cláusula de rescisão imotivada prevista no referido Contrato ou, caso tal disposição não exista, mediante notificação ao Google.

4.7 *Nenhuma Modificação nas SCCs.* O Contrato (incluindo este Aditivo) não tem como objetivo modificar ou contradizer as SCCs, nem prejudicar os direitos ou liberdades fundamentais dos titulares dos dados nos termos da Legislação Europeia de Proteção de Dados.

4.8 *Precedência das SSCs.* Na hipótese de qualquer conflito ou inconsistência entre as SCCs do Parceiro (incorporadas a este Aditivo por referência) e o restante do Contrato (incluindo este Aditivo), prevalecerão as SCCs do Parceiro.

5. Requisitos para o Envolvimento de Subprocessadores. A Legislação Europeia de Proteção de Dados exige que o Google assegure, por meio de contrato escrito, que as obrigações de proteção de dados descritas neste Aditivo, conforme previsto no Artigo 28(3) do GDPR, se aplicável, sejam impostas a quaisquer Subprocessadores contratados pelo Google.

CCPA

1. Definições Adicionais.

- *CCPA* refere-se à Lei de Privacidade do Consumidor da Califórnia de 2018, conforme alterada, incluindo as alterações introduzidas pela Lei de Direitos de Privacidade da Califórnia de 2020, juntamente com todos os regulamentos implementados.
- *Dados Pessoais do Parceiro* inclui as "informações pessoais".
- Os termos "empresa", "finalidade comercial", "consumidor", "informação pessoal", "tratamento", "venda", "vender", "fornecedor de serviço" e "compartilhamento" têm os significados atribuídos pela CCPA.

2. Proibições. Sem prejuízo das obrigações do Google nos termos da Seção 5.2 (Conformidade com as Instruções do Parceiro), no que diz respeito ao tratamento dos Dados Pessoais do Parceiro em conformidade com a CCPA, o Google não vai, salvo se de outro modo permitido pela CCPA:

a. Vender ou compartilhar os Dados Pessoais do Parceiro.

b. Reter, utilizar ou divulgar os Dados Pessoais do Parceiro:

i. Exceto se for para fins comerciais de acordo com a CCPA em nome do Parceiro e, especificamente, prestar os Serviços e o TSS;

ii. Fora do relacionamento comercial direto entre o Google e o Parceiro.

c. Combinar ou atualizar os Dados Pessoais do Parceiro com informações pessoais que o Google recebe de terceiros ou em nome deles, ou que coleta nas próprias interações com o consumidor.

3. Conformidade. Sem prejuízo das obrigações do Google de acordo com a Seção 5.2 (Conformidade com as Instruções do Parceiro) ou de outros direitos ou obrigações das partes previstas no Contrato, o Google notificará o Parceiro caso, na opinião do Google, não seja possível cumprir as obrigações nos termos da CCPA, salvo se tal notificação for proibida pela legislação aplicável.

4. Intervenção do Parceiro. Se o Google notificar o Parceiro sobre qualquer uso não autorizado dos Dados Pessoais do Parceiro, inclusive nos termos da Seção 3 (Conformidade) desta subseção ou da Seção 7.2.1 (Notificação de Incidentes), o Parceiro poderá adotar medidas razoáveis e apropriadas para cessar ou remediar tal uso não autorizado, incluindo:

a. Adotar quaisquer medidas recomendadas pelo Google nos termos da Seção 7.2.2 (Detalhes do Incidente de Dados), se aplicável.

b. Exercer seus direitos nos termos da Seção 7.5.2 (a. Auditoria do Parceiro) ou 9.1 (Acesso; Retificação; Tratamento Restrito; Portabilidade).

Turquia

1. Definições Adicionais.

- *Lei Turca de Proteção de Dados* refere-se à Lei Turca sobre a Proteção de Dados Pessoais n.º 6698, de 7 de abril de 2016.
- *Autoridade Turca de Proteção de Dados Pessoais* refere-se à Kişisel Verileri Koruma Kurumu.
- *SCCs turcas* refere-se às cláusulas contratuais padrão de acordo com a Lei de Proteção de Dados da Turquia.

2. Transferências de Dados.

2.1 *Termos Adicionais*. Se o endereço de cobrança do Parceiro estiver localizado na Turquia e o Google disponibilizar quaisquer termos adicionais opcionais (incluindo as SCCs turcas) para aceitação pelo Parceiro em relação à transferência de Dados Pessoais do Parceiro sob a Lei Turca de Proteção de Dados, tais termos complementarão este Aditivo a partir da data em que forem notificados à Autoridade Turca de Proteção de Dados Pessoais, conforme disposto na Seção 2.2 (Notificação à Autoridade Competente) abaixo, conforme comprovado pelo Parceiro ao Google.

2.2 *Notificação à Autoridade Competente*. Se o Parceiro sujeitar-se a SCCs da Turquia nos termos desta Seção 2 (Transferências de Dados), o Parceiro será responsável por notificar o uso das SCCs da Turquia à Autoridade Turca de Proteção de Dados Pessoais em até 5 (cinco) dias úteis após a assinatura das SCCs da Turquia, conforme exigência da Lei Turca de Proteção de Dados.

2.3 *Auditorias de SCC*. Se o Parceiro sujeitar-se a SCCs da Turquia nos termos desta Seção 2 (Transferências de Dados), o Google permitirá ao Cliente (ou a um auditor independente nomeado pelo Parceiro) a realização de auditorias segundo a descrição das SCCs e, durante a auditoria, disponibilizará todas as informações exigidas pelas SCCs, nos termos da Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

2.4 *Rescisão em Razão de Risco na Transferência de Dados*. Se o Parceiro concluir, com base em seu uso atual ou pretendido dos Serviços, que não estão sendo fornecidas salvaguardas adequadas para os Dados Pessoais do Parceiro transferidos, o Parceiro poderá rescindir imediatamente o Contrato aplicável, de acordo com a cláusula de rescisão imotivada prevista no referido Contrato ou, caso tal disposição não exista, mediante notificação ao Google.

2.5 *Sem Modificação a SCCs da Turquia*. O Contrato (incluindo este Aditivo) não tem como objetivo modificar ou contradizer as SCCs da Turquia, nem prejudicar os direitos ou liberdades fundamentais dos titulares dos dados nos termos da Lei Turca de Proteção de Dados.

2.6 *Precedência das SSCs.* Em caso de conflito ou inconsistência entre as SCCs da Turquia (que serão incorporadas por referência a este Aditivo em caso de celebração pelo Parceiro) e o restante do Contrato (incluindo este Aditivo), as SCCs da Turquia prevalecerão.

Israel

1. Definição Adicional.

- *Lei Israelense de Proteção de Privacidade* refere-se à Lei Israelense de Proteção de Privacidade de 1981 e eventuais regulamentos promulgados nos termos dessa lei.

2. Termos Equivalentes. Termos equivalentes a "controlador", "dados pessoais", "tratamento" e "processador", quando usados neste Aditivo, terão os significados estabelecidos pela Lei Israelense de Proteção de Privacidade.

3. Direitos de Auditoria do Parceiro. O Google permitirá que o Parceiro, ou auditor independente por ele indicado, realize auditorias (incluindo inspeções) conforme descrito na Seção 7.5.2 (a. Auditoria do Parceiro).

Brasil

1. **Definições Adicionais.**

- **"País Adequado"** significa, para dados processados de acordo com a LGPD, o Brasil ou um país ou organização internacional reconhecida pela Autoridade Nacional de Proteção de Dados (ANPD) como garantindo proteção adequada conforme a LGPD.
- **"Solução de Transferência Alternativa"** significa, para fins destes termos brasileiros, uma solução, diferente das Cláusulas Contratuais Padrão Brasileiras (BR SCCs), que permite a transferência internacional lícita de dados pessoais de acordo com a LGPD.
- **"BR SCCs"** significa as Cláusulas Contratuais Padrão Brasileiras (BR SCCs) (Controlador para Operador), as BR SCCs (Operador para Operador) ou as BR SCCs (Operador para Operador, Google Exportador), conforme aplicável.
- **"BR SCCs (Controlador para Operador)"** significa os termos em https://cloud.google.com/sccs/br-c2p?hl=pt-brXXXX.
- **"BR SCCs (Operador para Operador)"** significa os termos em https://cloud.google.com/sccs/br-p2p?hl=pt-brXXXX.
- **"BR SCCs (Operador para Operador, Google Exportador)"** significa os termos em https://cloud.google.com/sccs/br-p2p-intra-group?hl=pt-brXXXX.
- **"LGPD"** significa a Lei Brasileira nº 13.709/2018, conforme alterada.

2. **Notificações de Instrução.** Sem prejuízo das obrigações do Google sob a Seção 5.2 (Conformidade com as Instruções do Parceiro) ou quaisquer outros direitos ou obrigações de qualquer das partes sob o Contrato aplicável, o Google notificará imediatamente o Parceiro se, na opinião do Google:

a. A lei brasileira proibir o Google de cumprir uma Instrução;

b. Uma Instrução não estiver em conformidade com a LGPD; ou

c. O Google estiver de alguma outra forma impossibilitado de cumprir uma Instrução,

em cada caso, a menos que tal aviso seja proibido pela lei brasileira.

Se o Parceiro for um operador, o Parceiro encaminhará imediatamente ao controlador terceirizado qualquer aviso fornecido pelo Google sob esta seção.

3. **Transferência de Dados.**

3.1. Transferências Restritas. As partes reconhecem que a LGPD não exige BR SCCs ou uma Solução de Transferência Alternativa para que os Dados Pessoais do Parceiro sejam processados ou transferidos para um País Adequado. Se os Dados Pessoais do Parceiro forem transferidos para qualquer outro país e a LGPD se aplicar às transferências ("Transferências Restritas BR"), então:

a. Se o Google tiver adotado uma Solução de Transferência Alternativa para quaisquer Transferências Restritas BR, o Google informará o Parceiro sobre a solução relevante e garantirá que tais Transferências Restritas sejam feitas em conformidade com ela; ou

b. Se o Google não tiver adotado uma Solução de Transferência Alternativa para quaisquer Transferências Restritas BR, ou informar o Parceiro que o Google não está mais adotando uma Solução de Transferência Alternativa para quaisquer Transferências Restritas BR (sem adotar uma Solução de Transferência Alternativa de substituição):

i. Se o endereço do Google estiver em um País Adequado, as BR SCCs (Operador para Operador, Google Exportador) se aplicarão em relação a tais Transferências Restritas do Google para Suboperadores; ou

ii. Se o endereço do Google não estiver em um País Adequado, as BR SCCs (Controlador para Operador) ou BR SCCs (Operador para Operador) se aplicarão (dependendo se o Cliente é um controlador ou operador) em relação a tais Transferências Restritas entre o Google e o Parceiro.

3.2. Informações sobre Transferências Restritas. O Google fornecerá ao Parceiro informações relevantes sobre Transferências Restritas BR, Controles de Segurança Adicionais e outras medidas de proteção suplementares:

a. Conforme descrito na Seção 7.5.1 (Análises da Documentação de Segurança);

b. Em quaisquer locais adicionais descritos no Apêndice 4 (Produtos Específicos); e

c. Em relação à adoção pelo Google de uma Solução de Transferência Alternativa, em https://cloud.google.com/terms/alternative-transfer-solution.

3.3. BR SCCs e Controladores Terceirizados. Se o Parceiro for um operador, o Parceiro reconhece que o Google, como outro operador, pode não ser capaz de identificar o controlador terceirizado e, consequentemente, o Parceiro:

a. Encaminhará ao controlador terceirizado prontamente e sem atraso indevido qualquer aviso que se refira a quaisquer BR SCCs;

b. Será o único responsável, entre o Google e o Parceiro, por garantir a conformidade do controlador terceirizado com as obrigações de transparência sob as BR SCCs; e

c. Mediante solicitação por escrito do Google, fornecerá prontamente as seguintes informações sobre o controlador terceirizado: nome, detalhes corporativos (por exemplo, tipo de entidade, endereço registrado, identificador fiscal), endereço principal, endereço de email, ponto de contato do titular dos dados e [Alternativa: adicionar "(na medida permitida pelo contrato do Cliente com o controlador)"] quaisquer detalhes exigidos pelas BR SCCs em relação ao contrato do Cliente com o controlador.

3.4. Rescisão Devido a Risco de Transferência de Dados. Se o Parceiro concluir, com base em seu uso atual ou pretendido dos Serviços, que salvaguardas apropriadas não são fornecidas para os Dados Pessoais do Parceiro transferidos, o Parceiro poderá rescindir imediatamente o Contrato aplicável em conformidade com a cláusula de rescisão por conveniência desse Contrato ou, se não houver tal cláusula, notificando o Google.

3.5. Não Modificação das BR SCCs. Nada no Contrato (incluindo este Adendo) tem a intenção de modificar ou contradizer as BR SCCs.

3.6. Precedência das BR SCCs. Na medida de qualquer conflito ou inconsistência entre as BR SCCs (Controlador para Operador) e as BR SCCs (Operador para Operador) (que são incorporadas como anexos a este Adendo, conforme aplicável) e o restante do Contrato (incluindo este Adendo), as BR SCCs aplicáveis prevalecerão.

Apêndice 4: Produtos Específicos

Os termos em cada subseção do Apêndice 4 aplicam-se unicamente ao tratamento dos Dados do Parceiro pelos Serviços correspondentes.

Google Cloud Platform

1. Definições Adicionais.

- *Conta*, caso não seja definido no Contrato, refere-se à conta do Parceiro no Google Cloud Platform.

- *Google Cloud Platform* refere-se aos Serviços do Google Cloud Platform descritos em https://cloud.google.com/terms/services, excluindo Soluções de Terceiros.

- *Soluções de Terceiros*, caso não seja definido no Contrato, refere-se a (a) serviços, softwares, produtos e outros itens de terceiros que não sejam incorporados ao Google Cloud Platform ou ao Software, (b) soluções identificados na seção "Termos de Terceiros" dos Termos Específicos do Serviço do Contrato e (c) sistemas operacionais de terceiros.

2. Certificações de Conformidade. As Certificações de Conformidade dos Serviços Auditados do Google Cloud Platform também incluirão certificados de ISO 27017 e ISO 27018 e um Atestado de Conformidade PCI DSS.

3. Locais dos Data Centers. Os locais dos data centers do Google Cloud Platform são descritos em https://cloud.google.com/about/locations/.

4. Informações sobre Subprocessadores. Os nomes, os locais e as atividades dos Subprocessadores do Google Cloud Platform são descritos em https://cloud.google.com/terms/subprocessors.

5. Equipe de Proteção de Dados do Cloud. É possível entrar em contato com a Equipe de Proteção de Dados do Google Cloud Platform em https://support.google.com/cloud/contact/dpo.

6. Informações sobre Transferências Restritas. Informações adicionais relevantes sobre Transferências Restritas, Controles de Segurança Adicionais e outras medidas de proteção suplementares estão disponíveis em https://cloud.google.com/privacy.

7. Termos Específicos de Serviços.

Solução Bare Metal (Google Cloud Platform)

A Solução Bare Metal oferece acesso não virtualizado aos recursos da infraestrutura e tem certas características distintas desde a concepção.

1. Emendas. Este Aditivo tem as seguintes emendas em relação à Solução Bare Metal:

- A definição de "Auditor Terceirizado do Google" será substituída pelo seguinte:

    - *Auditor Terceirizado do Google* refere-se a um auditor terceirizado, independente, nomeado pelo Google ou por um Subprocessador da Solução Bare Metal, cuja identidade atual o Google informará ao Parceiro mediante solicitação.

- Os seguintes termos são excluídos:

    - Na Seção 7.1.1 (Medidas de Segurança do Google), os termos "Criptografar os Dados do Parceiro".

    - No Apêndice 2 (Medidas de Segurança), as subseções da Seção 1(a) intituladas "Sistemas Operacionais do Servidor" e "Continuidade de Negócios".

- No Apêndice 2, as subseções da Seção 1(b) intituladas "Superfície de Ataque Externa", "Detecção de Intrusões" e "Tecnologias de Criptografia".

- No Apêndice 2, as seguintes frases da Seção 3(a):

    - O Google armazena dados em ambiente multilocatário, em servidores de sua propriedade. De acordo com as instruções do Parceiro em contrário (por exemplo, na forma de uma seleção de local de dados), o Google replica os Dados do Parceiro entre os diversos data centers geograficamente dispersos."

2. Certificações de Conformidade e Relatórios SOC. O Google ou seu Subprocessador deverão manter, no mínimo, os seguintes itens (ou uma alternativa equivalente ou aprimorada) em referência à Solução Bare Metal, para comprovar a eficácia contínua das Medidas de Segurança:

a. Um certificado ISO 27001 e um Atestado de Conformidade PCI DSS (*Certificações de Conformidade BMS*).

b. Relatórios SOC 1 e SOC 2, atualizados anualmente, com base em uma auditoria realizada ao menos uma vez a cada 12 meses (*Relatórios BMS SOC*).

3. Revisões da Documentação de Segurança. Para demonstrar o cumprimento das obrigações nos termos deste Aditivo, o Google disponibilizará as Certificações de Conformidade BMS e os Relatórios BMS SOC para análise pelo Parceiro e, se o Parceiro for um processador, permitirá que o Parceiro solicite ao terceiro controlador o acesso aos Relatórios BMS SOC, nos termos da Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

4. Obrigações do Parceiro. Sem limitar as obrigações expressas do Google em relação à Solução Bare Metal, o Parceiro adotará medidas adequadas para proteger e manter a segurança dos Dados do Parceiro e de outros conteúdos armazenados em ou tratados por meio da Solução Bare Metal.

5. Exoneração de Responsabilidade. Não obstante qualquer disposição em contrário no Contrato (incluindo este Aditivo), o Google não é responsável por qualquer das seguintes situações em relação à Solução Bare Metal:

a. Segurança de outro tipo que não física, tais como controles de acesso, criptografia, firewalls, antivírus, detecção de ameaças e verificação de segurança.

b. Registro e Monitoramento.

c. Manutenção ou suporte para outros itens exceto hardware.

d. Backup dos dados, incluindo configurações de redundância ou de alta disponibilidade.

e. Políticas ou procedimentos de continuidade de negócios e de recuperação de desastres.

O Parceiro é exclusivamente responsável pela segurança (exceto a segurança física dos servidores da Solução Bare Metal), geração de registros e monitoramento, manutenção, suporte e backup de quaisquer Sistemas Operacionais, Dados do Parceiro, software e aplicativos que o Parceiro usa para uploads ou hospeda na Solução Bare Metal.

Cloud NGFW (Google Cloud Platform)

A edição do Cloud NGFW intitulada "Cloud NGFW Enterprise" ("CNE") foi projetada para reduzir o risco à cibersegurança e, portanto, tem certas características distintas.

1. Emendas. A seguinte alteração é feita ao Aditivo em relação ao CNE:

- As Seções 6.1 (Exclusão pelo Parceiro) e 6.2 (Devolução ou Exclusão ao Término da Vigência) não impedirão o Google nem Subprocessadores de reter eventuais arquivos ou captura de pacotes de tráfego de rede enviados para fins de SST e designados pelo CNE como uma ameaça de segurança, contanto que o arquivo ou a captura de pacote de tráfego de rede não inclua Dados Pessoais do Parceiro.

Google Distributed Cloud connected (Google Cloud Platform)

O Google Distributed Cloud connected não é implantado em data centers do Google e tem certas características distintas propositadamente.

1. Emendas. Este Aditivo tem as seguintes emendas em relação ao Google Distributed Cloud connected :

- A definição de “Incidente de Dados” é substituída pela seguinte:

  ‘“Incidente de Dados” significa uma violação da segurança do Google que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a Dados do Parceiro em sistemas gerenciados ou de outra forma controlados pelo Google, mas, para maior clareza, excluindo quaisquer violações relacionadas a hardware ou infraestrutura que sejam gerenciados, hospedados ou operados pelo Parceiro, ou de outra forma sob sua responsabilidade.’

- As referências a "sistemas do Google" são substituídas por "o Equipamento".

- A Seção 6.2 (Devolução ou Exclusão ao Término da Vigência) é substituída pelo seguinte:

  - 6.2 *Devolução ou Exclusão ao Término da Vigência*. O Parceiro instrui o Google a excluir todos os Dados remanescentes do Parceiro (incluindo cópias) do Equipamento no fim da Vigência de acordo com a legislação aplicável. Caso o Parceiro queira reter quaisquer Dados do Parceiro após o término da Vigência, poderá exportar ou fazer cópias desses dados antes do término da Vigência. O Google cumprirá a Instrução desta Seção 6.2 assim que seja razoavelmente viável e no período máximo de 180 dias, a menos que o armazenamento seja exigido pela Lei Europeia (em caso de sujeição à Lei Europeia de Proteção de Dados) ou pela lei aplicável (em caso de sujeição a outra Lei de Privacidade Aplicável).

- Adicionam-se as seguintes palavras ao final da Seção 10.1 (Instalações de Armazenamento e Tratamento de Dados): "ou no Local do Parceiro".

- Substitui-se a Seção 1 (Segurança de Redes e Data Centers) do Apêndice 2 (Medidas de Segurança) pelo seguinte texto:

    - **1. Máquinas Locais e Segurança de Rede**

Máquinas Locais. Os Dados do Parceiro serão armazenados exclusivamente no Equipamento a ser implantado no Local do Parceiro.

Sistemas Operacionais do Servidor. Os servidores do Google usam uma implementação baseada em Linux personalizada para o ambiente do aplicativo. O Google emprega um processo de revisão de código para aumentar a segurança do código usado para fornecer o Google Distributed Cloud connected e aprimorar os produtos de segurança nos ambientes de produção do Google Distributed Cloud connected .

Tecnologias de Criptografia. O Google disponibiliza a criptografia HTTPS (também chamada de conexão SSL ou TLS) e permite a criptografia de dados em trânsito. Os servidores do Google oferecem suporte à troca de chaves criptográficas Diffie-Hellman por meio de curvas elípticas efêmeras, assinadas com RSA e ECDSA. Esses métodos de perfect forward secrecy (PFS) contribuem para proteger o tráfego e minimizam o impacto em caso de comprometimento de uma chave ou de avanços em criptografia. O Google também disponibiliza a criptografia de dados em repouso, usando ao menos AES128 ou semelhante. O Google Distributed Cloud connected tem uma integração do CMEK. Encontre mais detalhes em https://cloud.google.com/kms/docs/cmek.

Conexão com o Cloud VPN. O Google permite ao Parceiro ativar e configurar uma interconexão forte e criptografada entre o Equipamento e a Nuvem Privada Virtual do Parceiro, usando o Cloud VPN por meio de uma conexão VPN IPSEC.

Armazenamento Vinculado. O armazenamento de dados do Parceiro está vinculado ao servidor. Em caso de furto de um disco ou cópia em repouso do disco, não será possível recuperar o conteúdo do disco fora do servidor.

- Excluem-se as Seções 2 (Controles de Acesso e Local) e 3 (Dados) do Apêndice 2 (Medidas de Segurança).

2. Disposições Inaplicáveis. As obrigações do Google estabelecidas no Contrato (incluído este Aditivo) ou em declarações na documentação de segurança associada (incluindo artigos) que dependam da operação por parte do Google de um data center próprio não se aplicam ao Google Distributed Cloud connected .

Multicloud Gerenciado pelo Google (Google Cloud Platform)

Os Serviços Multicloud Gerenciados pelo Google envolvem infraestrutura terceirizada e têm certas características distintas propositadamente.

1. Definição Adicional.

- *Aditivo sobre Tratamento de Dados do MCS Gerenciado pelo Google* refere-se aos termos disponíveis em https://cloud.google.com/terms/mcs-data-processing-terms.

2. Termos de Tratamento de Dados de Multicloud. O Aditivo sobre Tratamento de Dados do MCS Gerenciado pelo Google complementa e emenda o presente Aditivo em relação aos Serviços Multicloud Gerenciados pelo Google para o Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

É possível que o Google não tenha acesso ao ambiente do Parceiro no VMware ou não possa criptografar os dados pessoais no ambiente do Parceiro no VMware.

NetApp Volumes (Google Cloud Platform)

1. Emendas. Este Aditivo tem as seguintes emendas em relação a NetApp Volumes:

- A definição de "Auditor Terceirizado do Google" será substituída pelo seguinte:
    - *Auditor Terceirizado do Google* refere-se a um auditor terceirizado independente, nomeado pelo Google ou por um Subprocessador de NetApp Volumes, cuja identidade atual o Google informará ao Parceiro mediante solicitação.
- Substitui-se a Seção 3(a) (Armazenamento, Isolamento e Registro de Dados) do Apêndice 2 (Medidas de Segurança) pelo seguinte texto:
    - (a) *Armazenamento, Isolamento e Registro de Dados*. O Google armazena os dados em um ambiente com vários locatários, em servidores de propriedade da NetApp, Inc. Salvo eventuais Instruções em contrário (por exemplo, na forma da seleção de um local dos dados), o Google replicará os Dados do Parceiro entre data centers dispersos geograficamente. O Google também isola logicamente os Dados do Parceiro. O Parceiro receberá o controle de políticas específicas de compartilhamento de dados pessoais. Essas políticas, em conformidade com a funcionalidade dos Serviços, permitirão ao Parceiro determinar as configurações de compartilhamento de produtos aplicáveis aos Usuários Finais do Parceiro para finalidades específicas. O Parceiro pode optar por utilizar a geração de registros disponibilizada pelo Google por meio dos Serviços.

2. Certificações de Conformidade e Relatórios SOC. O Google ou seu Subprocessador obterá, no mínimo, os seguintes itens (ou uma alternativa equivalente ou aprimorada) em relação a NetApp Volumes:

a. Um certificado ISO 27001 e um Atestado de Conformidade PCI DSS (*Certificações de Conformidade NetApp*).

b. Relatórios SOC 1 e SOC 2, atualizados anualmente, com base em uma auditoria realizada, no mínimo, uma vez a cada 12 meses (*Relatórios NetApp SOC*).

3. 7.5.1 Revisões da Documentação de Segurança. Para demonstrar o cumprimento das obrigações nos termos deste Aditivo, o Google disponibilizará as Certificações de Conformidade NetApp e os Relatórios NetApp SOC para análise pelo Parceiro e, se o Parceiro for um processador, permitirá que o

Parceiro solicite ao terceiro controlador o acesso aos Relatórios NetApp SOC, nos termos da Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

Looker (original)

1. Definições Adicionais.

- *Admin Console* refere-se a qualquer console de administrador aplicável a cada instância.
- *Aditivo sobre Tratamento de Dados do MCS Gerenciado pelo Google* refere-se, se aplicável, aos termos disponíveis em https://cloud.google.com/terms/mcs-data-processing-terms.
- *Serviços Multicloud Gerenciados pelo Google* referem-se, se aplicável, aos serviços, produtos e recursos do Google especificados que são hospedados na infraestrutura de um provedor de nuvem terceirizado.
- *Looker (original)* significa uma plataforma integrada, incluindo infraestrutura baseada na nuvem (se aplicável) e componentes de software (incluindo APIs associadas) que permitem às empresas analisar dados e definir métricas comerciais em várias origens de dados, disponibilizadas pelo Google ao Parceiro nos termos do Contrato. Looker (original) exclui Produtos de Terceiros.
- *Provedor Terceirizado de Serviço Multicloud* " terá o significado que consta no Aditivo sobre Tratamento de Dados do MCS Gerenciado pelo Google.
- *Formulário de Pedido* terá o significado constante no Contrato, a menos que o Parceiro tenha comprado por meio de um revendedor ou marketplace on-line ou esteja usando o Looker apenas para fins de teste ou avaliação sujeito a um contrato de teste ou de avaliação, caso em que Formulário de Pedido poderá referir-se a outro formulário escrito (incluindo e-mail ou outro meio eletrônico) se autorizado pelo Google.

2. Emendas. Este Aditivo tem as seguintes emendas em relação ao Looker (original):

- Substitui-se a definição de "Endereço de E-mail de Notificação" pelo seguinte texto:
    - *Endereço de E-mail de Notificação* refere-se aos endereços de e-mail designados pelo Parceiro no Formulário do Pedido ou no Looker (conforme o caso) para receber determinadas notificações do Google.
- Substituem-se as definições de "SCCs (Controlador para Operador)", "SCCs (Operador para Controlador)", "SCCs (Operador para Operador)" e "SCCs (Operador para Operador, Exportador do Google)", no Apêndice 3 (Leis de Privacidade Específicas) pelo seguinte texto:
    - *SCCs (Controlador para Operador)* refere-se aos termos disponíveis em: https://cloud.google.com/terms/looker/legal/sccs/eu-c2p
    - *SCCs (Operador para Controlador)* refere-se aos termos disponíveis em: https://cloud.google.com/terms/looker/legal/sccs/eu-p2c.

- *SCCs (Operador para Operador)* refere-se aos termos disponíveis em: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p.

- *SCCs (Operador para Operador, Exportador do Google)* refere-se aos termos disponíveis em: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group.

- Adicionam-se as seguintes palavras ao final da Seção 10.1 (Instalações de Armazenamento e Tratamento de Dados): "ou onde algum Provedor Terceirizado de Serviço Multicloud tenha instalações".

3. Responsabilidades Adicionais de Segurança do Parceiro. O Parceiro é responsável pela segurança do seu próprio ambiente, bancos de dados e configurações do Looker (original), excluindo os sistemas gerenciados e controlados pelo Google.

4. Certificações de Conformidade e Relatórios SOC. As Certificações de Conformidade e Relatórios SOC para Serviços Auditados do Looker (original) podem diferir dependendo do ambiente de hospedagem em que são usados os Serviços relevantes. O Google informará, mediante solicitação, os detalhes das Certificações de Conformidade e Relatórios SOC disponíveis referentes aos ambientes de hospedagem específicos.

5. Locais dos Data Centers. Os locais dos data centers do Looker (original) serão relacionados no Formulário de Pedido aplicável ou identificados de outra forma pelo Google.

6. Sem Certificação para Parceiros Fora da EMEA. O Parceiro não tem a obrigação de certificar ou identificar sua Autoridade Supervisora competente, nos termos da Seção 4.2 (Certificação por Parceiros Fora da EMEA), dos termos de Proteção de Dados da Europa no Apêndice 3 (Leis de Privacidade Específicas) para o Looker (original).

7. Informações sobre Transferências Restritas. Informações adicionais relevantes sobre Transferências Restritas, Controles de Segurança Adicionais e outras medidas de proteção suplementares do Looker (original) estão disponíveis em https://docs.looker.com.

8. Informações sobre Subprocessadores. Os nomes, os locais e as atividades dos Subprocessadores do Looker (original) são descritos em:

a. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors.

b. https://cloud.google.com/terms/subprocessors.

9. Multicloud Gerenciado pelo Google (Looker (original))

Os Serviços Multicloud Gerenciados pelo Google envolvem infraestrutura terceirizada e têm certas características distintas propositadamente.

9.1 *Termos de Tratamento de Dados de Multicloud*. O Aditivo sobre Tratamento de Dados do MCS Gerenciado pelo Google complementa e emenda o presente Aditivo em relação aos Serviços Multicloud Gerenciados pelo Google para o Looker (original).

10. Equipe de Proteção de Dados do Cloud. É possível entrar em contato com a Equipe de Proteção de Dados do Looker (original) em https://support.google.com/cloud/contact/dpo.

11. Registros de Tratamento do Google. Na medida em que alguma Lei de Privacidade Aplicável exigir que o Google colete e mantenha registros de certas informações relacionadas ao Parceiro ou os Clientes dele, o Parceiro fornecerá tais informações ao Google, mediante solicitação, e notificará o Google sobre eventuais alterações necessárias para manter as informações corretas e atualizadas, a menos que o Google solicite que o Parceiro forneça e atualize tais informações por outros meios.

12. Medidas de Segurança Adicionais do Aplicativo. O Google implementará e manterá, para o Looker (original), as Medidas de Segurança Adicionais descritas abaixo:

a. O Google segue, no mínimo, os padrões do setor para arquitetura de segurança. Para proteger o acesso ao Looker, os servidores de proxy usados pelos aplicativos do Google atuam como um ponto único para a filtragem de ataques com lista de bloqueio de IPs e limitação de taxa de conexão.

b. Os administradores do Parceiro controlam o acesso dos funcionários do Google aos aplicativos para prestar o suporte técnico solicitado pelo Parceiro ou pelos Usuários Finais.

Serviços de SecOps

1. Definições Adicionais.

- *Conta*, caso não seja definido no Contrato, refere-se à conta do Parceiro nos Serviços de SecOps ou no Google Cloud Platform, conforme o caso.
- *Serviços de SecOps* refere-se às Soluções do Chronicle SIEM, do Chronicle SOAR e da Mandiant, cada um conforme descrito em https://cloud.google.com/terms/secops/services, exceto Soluções de Terceiros. Para evitar dúvidas, os Serviços de SecOps não incluem os Serviços Gerenciados da Mandiant nem os Serviços de Consultoria da Mandiant.
- *Soluções de Terceiros*, caso não seja definido no Contrato, refere-se a (a) serviços, softwares, produtos e outras soluções de terceiros que não foram incorporados aos Serviços de SecOps ou ao Software e (b) sistemas operacionais de terceiros.

2. Emendas. Este Aditivo tem as seguintes emendas em relação aos Serviços de SecOps:

- A definição de "Controles de Segurança Adicionais" foi substituída pelo seguinte texto:
    - *Controles de Segurança Adicionais* refere-se a recursos, funcionalidades e/ou controles de segurança que o Parceiro possa vir a usar, a seu critério e/ou por sua determinação, incluindo (se houver) criptografia, registros, monitoramento, gerenciamento de identidade e acesso e verificação de segurança.
-

- Substituem-se as definições de "SCCs (Controlador para Operador)", "SCCs (Operador para Controlador)", "SCCs (Operador para Operador)" e "SCCs (Operador para Operador, Exportador do Google)", no Apêndice 3 (Leis de Privacidade Específicas) pelo seguinte texto:

    - *SCCs (Controlador para Processador)* refere-se aos termos em: https://cloud.google.com/terms/secops/sccs/eu-c2p.

    - *SCCs (Processador para Controlador)* refere-se aos termos disponíveis em: https://cloud.google.com/terms/secops/sccs/eu-p2c.

    - *SCCs (Processador para Processador)* refere-se aos termos disponíveis em: https://cloud.google.com/terms/secops/sccs/eu-p2p.

    - *SCCs (Processador para Processador, Exportador do Google)* refere-se aos termos em: https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter.

3. Locais dos Data Centers. Os locais dos data centers de Serviços de SecOps são descritos em https://cloud.google.com/terms/secops/data-residency.

4. Sem Certificação para Parceiros Fora da EMEA. O Parceiro não tem a obrigação de certificar ou identificar sua Autoridade Supervisora competente, nos termos da Seção 4.2 (Certificação por Parceiros Fora da EMEA), dos termos de Proteção de Dados da Europa no Apêndice 3 (Leis de Privacidade Específicas) para os Serviços de SecOps.

5. Informações sobre Subprocessadores. Os nomes, os locais e as atividades dos Subprocessadores dos Serviços de SecOps estão disponíveis em https://www.google.com/about/datacenters/locations/

6. Equipe de Proteção de Dados do Cloud. É possível entrar em contato com a Equipe de Proteção de Dados dos Serviços de SecOps em https://support.google.com/cloud/contact/dpo (e/ou por outros meios que o Google venha a oferecer periodicamente).

7. Registros de Tratamento do Google. Na medida em que alguma Lei de Privacidade Aplicável exigir que o Google colete e mantenha registros de certas informações relacionadas ao Parceiro, o Parceiro fornecerá tais informações ao Google, mediante solicitação, e notificará o Google sobre eventuais alterações necessárias para manter as informações corretas e atualizadas, a menos que o Google solicite que o Parceiro forneça e atualize tais informações por outros meios.

Versões anteriores dos Termos de Tratamento e Segurança de Dados (Parceiro):

30 de junho de 2022 24 de setembro de 2021 20 de agosto de 2020 10 de agosto de 2020 17 de julho de 2020 1º de outubro de 2019 28 de fevereiro de 2019 25 de maio de 2018 13 de março de 2018

Versões anteriores de DPST de Serviços de SecOPs (Parceiros):

6 de fevereiro de 2023 31 de outubro de 2022 27 de setembro de 2021

Versões anteriores *(última modificação em 21 de agosto de 2025)*

15 de outubro de 2024 26 de setembro de 2024 9 de setembro de 2024 9 de abril de 2024 8 de novembro de 2023 15 de agosto de 2023 20 de setembro de 2022