Aditivo sobre Tratamento de Dados do Cloud (clientes)

O presente Aditivo sobre Tratamento de Dados do Cloud (incluindo seus apêndices, o "*Aditivo*") é incorporado ao Contrato entre o Google e o Cliente (definido abaixo). O Aditivo era chamado "Termos de Tratamento e Privacidade de Dados" em um Contrato do Google Cloud Platform, Looker (original), Serviços Google SecOps ou Google Cloud Skills Boost para Organizações; como "Aditivo sobre Tratamento de Dados" em um Contrato do Google Workspace ou do Cloud Identity; e como "Aditivo sobre Tratamento de Dados" em um Contrato de Serviços de Consultoria da Mandiant e de Serviços Gerenciados.

Termos Gerais

1. Visão Geral

O presente Aditivo estabelece 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 Cliente (segundo a definição abaixo). O Aditivo começa a valer a partir do Início da Vigência do Aditivo (definido abaixo) e substituirá quaisquer termos anteriormente aplicáveis ao tratamento e à segurança dos Dados do Cliente. Os termos em maiúsculas usados, mas não definidos neste Aditivo têm os significados definidos no Contrato.

2. Definições

2.1 Neste Aditivo:

- *Início da Vigência do Aditivo* significa a data em que o Cliente aceitou este Aditivo ou em que as partes, por outro meio, acordaram quanto à vigência dele.
- *Controles Adicionais de Segurança* se refere a recursos, funcionalidades e controles de segurança que o Cliente pode utilizar a critério exclusivo dele, incluindo o Admin Console, criptografia, geração de registros 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 Cliente.
- *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 Cliente. 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* se refere 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 URL, a menos que tenham sido descontinuados de acordo com o Contrato aplicável.

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

- *Dados do Cliente*, caso não seja definido no Contrato, terá a definição que consta no Apêndice 4 (Produtos Específicos).

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

- *Incidente de Dados*: significa uma violação da segurança do Google que gera destruição, perda, alteração, divulgação não autorizada de ou acesso acidentais ou ilegais a Dados do Cliente em sistemas gerenciados ou controlados pelo Google.

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

- *GDPR da União Europeia* se refere 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.

- *Legislação 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 Cliente); (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 Cliente); ou (c) a legislação suíça (caso a FADP da Suíça se aplique ao tratamento dos Dados Pessoais do Cliente).

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

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

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

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

- *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* se refere 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 Cliente para prestar partes dos Serviços e SSTs (se aplicável).
- *Autoridade Supervisora* significa, conforme aplicável: (a) uma autoridade supervisora, conforme definição no GDPR da UE; ou (b) o Comissário, conforme definição no GDPR do Reino Unido e/ou na FADP da Suíça.
- *FADP da Suíça* se refere, 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* se refere 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

Independentemente de o Contrato aplicável ter sido rescindido ou ter expirado, este Aditivo permanecerá em vigor até que o Google exclua todos os Dados do Cliente, conforme descrito neste Aditivo. Quando isso acontecer, eles expirarão automaticamente.

4. Funções; Conformidade Legal

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

4.2 *Resumo do Tratamento*. O objeto em questão e os detalhes do tratamento dos Dados Pessoais do Cliente 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 Cliente, nos termos da Lei de Privacidade Aplicável.

4.4 *Outros Termos Legais*. Na medida em que o tratamento dos Dados Pessoais do Cliente 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 *Clientes Operadores*. Se o Cliente for um operador:

a. O Cliente garante, de maneira contínua, que o terceiro controlador relevante autorizou:

i. As instruções

ii. O envolvimento do Google pelo Parceiro como outro operador; e

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

b. O Cliente encaminhará ao terceiro controlador relevante, prontamente e sem atraso, eventuais avisos enviados pelo Google nos termos da Seção 7.2.1 (Notificação de Incidentes), 9.2.1 (Responsabilidades pelas Solicitações) ou 11.4 (Direito de Oposição a Subprocessadores); e

c. O Cliente poderá disponibilizar ao terceiro controlador quaisquer outras informações disponibilizadas pelo Google nos termos deste Aditivo sobre a localização dos data centers do Google ou o nome, a localização e as atividades dos Subprocessadores

5.2 *Conformidade com as Instruções do Cliente*. O Cliente instrui o Google a processar os Dados do Cliente de acordo com o Contrato aplicável (incluindo este Aditivo) apenas da seguinte maneira:

a. A fim de oferecer, proteger e monitorar os Serviços e SST (se aplicável); e

b. Conforme especificado em maiores detalhes:

i. Pelo uso dos Serviços por parte do Cliente (incluindo via Admin Console) e SST (se aplicável); e

ii. Em outras instruções escritas fornecidas pelo Cliente 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 Legislação 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 Cliente*. O Google permitirá que o Cliente exclua os Dados do Cliente durante a Vigência de maneira consistente com a funcionalidade dos Serviços. Se o Cliente usar os Serviços para excluir quaisquer Dados do Cliente durante a Vigência e o Cliente não puder recuperar esses Dados do Cliente, esse uso constituirá uma instrução para o Google excluir os Dados do Cliente pertinentes 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 Legislação 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 quiser reter Dados do Cliente ao fim da Vigência, o Cliente poderá instruir o Google, nos termos da Seção 9.1 (Acesso, Retificação, Tratamento Restrito e Portabilidade), a devolver os dados durante a Vigência. Nos termos da Seção 6.3 (Instrução de Exclusão Tardia), o Cliente instrui o Google a excluir todos os Dados do Cliente restantes (incluindo cópias) dos sistemas do Google ao final 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 Legislação Europeia de Proteção de Dados) ou se a legislação relevante exigir a retenção (quando outra Lei de Privacidade Aplicável for pertinente).

6.3. *Instrução de Exclusão Tardia*. Em caso de tratamento de Dados do Cliente cobertos pela instrução de exclusão estabelecida na Seção 6.2 (Devolução ou Exclusão ao Término da Vigência), quando a Vigência em questão nos termos da Seção 6.2 expirar, em relação a um Contrato com Vigência contínua, tal instrução de exclusão terá efeito com relação a tais Dados do Cliente apenas quando a Vigência contínua expirar. Para fins de esclarecimento, o presente Aditivo continuará se aplicando a tais Dados do Cliente até sua exclusão pelo Google.

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 Cliente 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 Cliente 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 Cliente 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 Cliente 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; e

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

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

a. possibilitar que o Cliente proteja os Dados do Cliente; e

b. fornecer ao Cliente informações sobre como proteger, acessar e usar os Dados do Cliente.

7.1.4 *Assistência de Segurança do Google*. O Google, considerando a natureza do tratamento dos Dados Pessoais do Cliente e as informações disponíveis ao Google, ajudará o Cliente no cumprimento das próprias obrigações (ou, quando o Cliente for operador, das obrigações do respectivo 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 Adicionais de Segurança, conforme estabelecido na Seção 7.1.3 (Controles Adicionais de Segurança);

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 dará as informações contidas no Contrato aplicável (inclusive neste Aditivo); e

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

7.2 *Incidentes de Dados*.

7.2.1 *Notificação de Incidentes*. O Google notificará o Cliente, 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 Cliente.

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 Cliente 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 Cliente para lidar com o Incidente de Dados; e os

detalhes de um ponto de contato para conseguir mais informações. Se não for possível dar 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 Cliente Feita pelo Google*. O Google não tem a obrigação de avaliar os Dados do Cliente 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 um reconhecimento por parte do Google de qualquer falha ou responsabilidade em relação ao Incidente de Dados.

7.3 *Responsabilidades e Avaliação de Segurança do Cliente*.

7.3.1 *Responsabilidades de Segurança do Cliente*. Sem prejuízo das obrigações do Google estabelecidas nas Seções 7.1 (Medidas de Segurança, Controles e Assistência do Google) e 7.2 (Incidentes de Dados) e em outros trechos do Contrato aplicável, o Cliente é responsável pelo próprio uso dos Serviços e pelo eventual armazenamento de cópias dos Dados do Cliente fora dos sistemas do Google ou do Subprocessador do Google, incluindo:

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

b. Proteção das credenciais de autenticação de contas, sistemas e dispositivos que o Cliente usa para ter acesso aos Serviços; e

c. Backup ou retenção de cópias dos Dados do Cliente, quando apropriado.

7.3.2 *Avaliação de Segurança do Cliente*. O Cliente concorda que os Serviços, as Medidas de Segurança, os Controles Adicionais de Segurança e os compromissos assumidos pelo Google nos termos da Seção 7 (Segurança de Dados) proporcionam um nível de segurança apropriado ao risco relacionado aos Dados do Cliente (levando em consideração as tecnologias mais recentes, os custos de implementação, a natureza, o escopo, o contexto e as finalidades do tratamento dos Dados do Cliente, 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 quaisquer certificações adicionais descritas no Apêndice 4 (Produtos Específicos), as *Certificações de Conformidade*; e

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 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 suas obrigações nos termos deste Aditivo, o Google disponibilizará a Documentação de Segurança para revisão do Cliente e, caso o Cliente seja operador, o Google permitirá que o Cliente solicite acesso aos Relatórios SOC para o terceiro controlador relevante, em conformidade com a Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

7.5.2 *Direitos de Auditoria do Cliente*.

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

b. *Análise independente do cliente*. O Cliente pode realizar uma auditoria para verificar a conformidade do Google com suas obrigações estabelecidas neste Aditivo, analisando a Documentação de Segurança (que reflete o resultado das auditorias realizadas pelo Auditor Terceirizado do Google).

7.5.3 *Termos Comerciais Adicionais para Revisões e Auditorias*

a. O Cliente deverá entrar em contato com a Equipe de Proteção de Dados do Cloud do Google para solicitar:

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

ii. Uma auditoria nos termos da Seção 7.5.2(a) (Auditoria do Cliente).

b. Após uma solicitação do Cliente nos termos da Seção 7.5.3(a), o Google e o Cliente discutirão e concordarão nos seguintes pontos:

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

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

c. O Google poderá cobrar uma taxa, com base nos custos razoáveis que tenha, por qualquer auditoria realizada nos termos da Seção 7.5.2(a) (Auditoria do Cliente). O Google fornecerá ao Cliente mais detalhes sobre qualquer taxa aplicável e sobre a base de cálculo antes de auditorias desse tipo. O Cliente será responsável por quaisquer taxas cobradas por qualquer auditor designado pelo Cliente para executar tal auditoria.

d. O Google poderá se opor, por escrito, a um auditor nomeado pelo Cliente para realizar qualquer auditoria nos termos da Seção 7.5.2(a) (Auditoria do Cliente), 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 Cliente indique outro auditor ou conduza a auditoria por conta própria.

e. Quaisquer solicitações do Cliente 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 relevante ou à realização de auditorias também estarão sujeitas a esta Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

8. Avaliações de Impacto e Consultas

O Google vai, levando em consideração a natureza do tratamento e as informações disponíveis ao Google, auxiliar o Cliente na conformidade com suas obrigações (ou, quando o Cliente 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 Adicionais de Segurança nos termos da Seção 7.1.3 (Controles Adicionais de Segurança) e a Documentação de Segurança nos termos da Seção 7.5.1 (Revisões da Documentação de Segurança).

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

c. Se as subseções (a) e (b) acima forem insuficientes para que o Cliente (ou o terceiro controlador) cumpra tais obrigações, o Google, mediante solicitação do Cliente, vai cooperar e prestar assistência adicionais razoáveis.

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

9.1 *Acesso, Retificação, Tratamento Restrito e Portabilidade*. Durante a Vigência, o Google permitirá que o Cliente, de acordo com a funcionalidade dos Serviços, acesse, retifique e restrinja o tratamento dos Dados do Cliente, inclusive por meio da funcionalidade de exclusão fornecida pelo Google, descrita na Seção 6.1 (Exclusão pelo Cliente), bem como exporte os Dados do Cliente. Caso identifique que os Dados do Cliente estão incorretos ou desatualizados, o Cliente será o único responsável por usar tal funcionalidade para corrigir 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 do Cloud do Google receba uma solicitação de um titular de dados relacionada a Dados Pessoais do Cliente e que identifique o Cliente, o Google fará o seguinte:

a. Orientar o titular de dados a encaminhar a solicitação ao Cliente.

b. Informar prontamente ao Cliente.

c. Não responder a tal solicitação do titular de dados sem autorização do Cliente.

O Cliente deverá responder a tais solicitações, inclusive, quando necessário, utilizando a funcionalidade dos Serviços.

9.2.2 *Assistência a Solicitações de Titulares de Dados do Google*. O Google vai, levando em consideração a natureza do tratamento dos Dados Pessoais do Cliente, auxiliar o Cliente no cumprimento de suas obrigações (ou, quando o Cliente 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. Para isso, o Google fará o seguinte:

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

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 Cliente (ou o terceiro controlador) cumpra tais obrigações, o Google, mediante solicitação do Cliente, vai cooperar e prestar assistência adicionais razoáveis.

10. Locais de Tratamento de Dados

10.1 *Armazenamento de Dados e Instalações de Tratamento*. 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 Cliente poderão ser tratados em qualquer país onde o Google ou seus Subprocessadores 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 Cliente autoriza expressamente o Google a contratar como Subprocessadores as entidades informadas nos termos da 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 Cliente 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 Cliente na medida necessária para o cumprimento das obrigações a ele subcontratadas, e o fará em conformidade com o Contrato aplicável (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 algum Novo Subprocessador durante a Vigência, notificará o Cliente da contratação (incluindo o nome, a localidade e as atividades do Novo Subprocessador) no mínimo 30 dias antes do início do tratamento dos Dados do Cliente pelo Novo Subprocessador.

b. O Cliente poderá, no prazo de 90 dias após ser notificado da contratação de um Novo Subprocessadormanifestar sua oposição mediante a rescisão imotivada imediata do Contrato aplicável da seguinte forma:

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

ii. Caso não exista tal previsão, por notificação ao Google.

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

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 Cliente relacionados ao tratamento dos Dados do Cliente, nos termos do Contrato aplicável, podendo ser consultada conforme previsto na seção de Notificações do Contrato aplicável ou no Apêndice 4 (Produtos Específicos).

12.2 *Registros de Tratamento do Google.* O Google manterá a documentação adequada de suas atividades de tratamento, 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 Cliente, caberá ao Cliente 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 aos reguladores competentes, incluindo uma Autoridade Supervisora, 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 Cliente, o Google orientará esse terceiro a entrar em contato com o Cliente.

13. Notificações

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

Para fins de esclarecimento, se o Cliente tiver mais de um Contrato, este Aditivo alterará cada Contrato separadamente.

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

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

Objeto em Questão

A prestação dos Serviços e do SST (se aplicável) ao Cliente por parte do Google.

Duração do Tratamento

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

Natureza e Finalidade do Tratamento

O Google tratará os Dados Pessoais do Cliente para fins de fornecimento de Suporte e SST (se for o caso) ao Cliente, nos termos deste Aditivo.

Categorias de Dados

Dados relacionados a indivíduos fornecidos ao Google por meio dos Serviços pelo Cliente ou sob orientação deste ou pelos Usuários Finais do Cliente.

Titulares dos Dados

Os titulares dos dados incluem os indivíduos sobre os quais os dados são fornecidos ao Google por meio dos Serviços pelo Cliente (ou por orientação deste) ou pelos Usuários Finais do Cliente.

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 mantém data centers distribuídos geograficamente. 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 documentaram procedimentos de manutenção preventiva que detalham o processo e a frequência de desempenho de acordo com as especificações internas ou do fabricante. A manutenção preventiva 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. Uma alimentação de reserva é fornecida por vários mecanismos, por exemplo, baterias de fonte de alimentação ininterrupta (UPS, na sigla em inglês), que oferecem proteção elétrica consistentemente confiável durante blecautes parciais da concessionária de serviços públicos, blecautes, sobretensão/subtensão e condições de frequência fora da tolerância. 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 reserva. 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 reservados 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 desenvolveu e planeja e testa regularmente programas para recuperação de desastres/planejamento de continuidade de 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 data centers. 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. O Google considera os possíveis vetores de ataque e incorpora tecnologias específicas adequadas à proteção de sistemas expostos externamente.

Detecção de Intrusões. A detecção de intrusões fornece informações sobre atividades de ataque em andamento e informações adequadas para responder a incidentes. A detecção de intrusões do Google envolve (i) um rigoroso controle do tamanho e da composição da superfície de ataque, utilizando medidas preventivas (ii) controles inteligentes de detecção nos pontos de entrada de dados, e (iii) a 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 de Diffie-Hellman por meio de curvas elípticas efêmeras, assinadas com criptografia 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 e 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 chave eletrônica, com alarmes conectados à equipe de segurança no local. Todas as pessoas que entram no data center são obrigadas a se identificar e mostrar um comprovante de identidade para a equipe de operações de segurança local. Somente funcionários, prestadores de serviço e visitantes devidamente autorizados podem ingressar nos data centers. Somente funcionários e contratados devidamente autorizados podem solicitar o acesso por chave eletrônica a essas instalações. As solicitações de acesso por chave eletrônica ao data center precisam 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 precisam: (i) conseguir 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 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 a chave eletrônica de cada indivíduo e quando ele acessa as portas de perímetro, a área de envio/recebimento e outras áreas críticas. Atividades não autorizadas e tentativas de acesso malsucedidas 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 nos data centers estão dotadas de 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 gerencia os equipamentos de monitoramento, gravação e controle do CCTV. Todos os data centers têm cabeamento seguro para conectar os equipamentos de CCTV. As câmeras realizam gravações contínuas do local com 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 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 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 e os Usuários Finais do Cliente precisam se autenticar por um sistema central de autenticação ou de um sistema de logon único para utilizar os Serviços.

Políticas e Processos Internos de Acesso aos Dados — Política de Acesso. Os processos e políticas de acesso aos dados internos do Google são projetados para evitar que pessoas e sistemas não autorizados consigam acesso a sistemas usados para tratar os Dados do Cliente. O Google projeta os sistemas para (i) permitir que apenas pessoas autorizadas acessem os dados que estão autorizadas a acessar; e (ii) garantir que os Dados do Cliente 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 IDs do 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 se baseia nas responsabilidades da função, nos requisitos das obrigações profissionais necessárias para realizar tarefas autorizadas e na necessidade de saber da equipe autorizada. 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 um ambiente multilocatário em servidores pertencentes a ele. Observadas eventuais Instruções em sentido contrário (por exemplo, quanto à seleção da localização dos dados), o Google replica os Dados do Cliente entre diversos data centers em várias regiões. O Google também faz o isolamento lógico dos Dados do Cliente. O Cliente receberá o controle sobre políticas específicas de compartilhamento de dados pessoais. Essas políticas, em conformidade com a funcionalidade dos Serviços, permitirão ao Cliente determinar as configurações de compartilhamento de produtos aplicáveis aos Usuários Finais do Cliente para finalidades específicas. O Cliente 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 Disco") 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 Disco.

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 adequadas de histórico para contratação, dentro do legalmente permitido e de acordo com as leis trabalhistas locais e regulamentações estatutárias aplicáveis.

A equipe do Google 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. É necessário que os funcionários que lidam com Dados do Cliente preencham requisitos adicionais apropriados à sua função (por exemplo, certificações). A equipe do Google não tratará os Dados do Cliente sem autorização.

5. Segurança do Subprocessador

Antes da integração de Subprocessadores, 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 Cliente.

Legislação Europeia de Proteção de Dados

1. Definições Adicionais.

- *País Adequado* se refere 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 de 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, para efeitos destes termos da Lei Europeia de Proteção de Dados,* significa 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 oferecem proteção adequada.

- *SCCs do Cliente* refere-se a SCCs (Controlador para Operador), SCCs (Operador para Operador) ou SCCs (Operador para Controlador), conforme aplicável.

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

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

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

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

- *SCCs (Operador para Operador, 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 Seção 5.2 (Conformidade com as Instruções do Cliente) ou de quaisquer outros direitos ou obrigações de qualquer das partes previstas no Contrato, o Google compromete-se a notificar imediatamente o Cliente 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. O Google não possa cumprir a Instrução por algum outro motivo.

Nos casos acima, apenas quando tal aviso não seja proibido pela Legislação Europeia.

Se o Cliente for um operador, o Cliente encaminhará imediatamente ao terceiro controlador relevante os avisos enviados pelo Google nos termos desta seção.

3. Direitos de Auditoria do Cliente. O Google permitirá que o Cliente ou um auditor independente nomeado pelo Cliente realizem auditorias (incluindo inspeções), nos termos da Seção 7.5.2(a) (Auditoria do Cliente). 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 Cliente sejam tratados ou transferidos para um País Adequado. Se os Dados Pessoais do Cliente forem transferidos para qualquer outro país e a Legislação Europeia de Proteção de Dados for aplicável a essas transferências, conforme certificado pelo Cliente nos termos da Seção 4.2 (Certificação por Clientes 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 Cliente 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 Cliente 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 (Operador para Operador, Exportador do Google) serão aplicáveis em relação a essas Transferências Restritas do Google para Subprocessadores.

B. Além disso, caso o endereço de cobrança do Cliente não esteja em um País Adequado, as SCCs (Operador para Controlador) serão aplicáveis (independentemente de o Cliente atuar como controlador ou operador) em relação a tais Transferências Restritas entre o Google e o Cliente.

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

4.2 *Certificação por Clientes Fora da EMEA*. Se o endereço de cobrança do Cliente estiver fora da EMEA e o tratamento dos Dados Pessoais do Cliente estiver sujeito à Legislação Europeia de Proteção de Dados, então, salvo indicação em contrário no Apêndice 4 (Produtos Específicos) deste Aditivo, o Cliente 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 Cliente informações relevantes sobre Transferências Restritas, Controles Adicionais de Segurança 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 SCCs do Cliente 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 Cliente (ou um auditor independente por ele designado) faça auditorias conforme previsto nessas SCCs e, durante a auditoria, todas as informações exigidas por essas SCCs, em conformidade com a Seção 7.5.3 (Termos Comerciais Adicionais para Revisões e Auditorias).

4.5 *Notificações de SCCs e terceiros Controladores*. Se o Cliente é um operador, o Cliente reconhece que o Google, como outro operador, pode não ser capaz de identificar o terceiro Controlador e, consequentemente, o Cliente encaminhará ao terceiro controlador , de forma imediata e sem atraso injustificado, qualquer notificação que faça referência a quaisquer SCCs.

4.6 *Rescisão em Razão de Risco na Transferência de Dados*. Se o Cliente concluir, com base em seu uso atual ou planejado dos Serviços, que não estão sendo fornecidas salvaguardas adequadas para os Dados Pessoais do Cliente transferidos, o Cliente 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 Cliente (incorporadas a este Aditivo por referência) e o restante do Contrato (incluindo este Aditivo), prevalecerão as SCCs do Cliente.

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 e suas alterações, incluindo as alterações introduzidas pela Lei de Direitos de Privacidade da Califórnia de 2020, juntamente com todos os regulamentos implementados.

- *Dados Pessoais do Cliente* inclui as "informações pessoais".

- Os termos "empresa", "finalidade comercial", "consumidor", "informação pessoal", "tratamento", "venda", "vender", "provedor de serviços" 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 Cliente), no que diz respeito ao tratamento dos Dados Pessoais do Cliente 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 Cliente.

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

i. Exceto se for para fins comerciais de acordo com a CCPA em nome do Cliente e, especificamente, prestar os Serviços e SST (se for o caso);

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

c. Combinar ou atualizar os Dados Pessoais do Cliente com informações pessoais que o Google receba de terceiros ou em nome deles, ou que colete 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 Cliente) ou de outros direitos ou obrigações das partes previstas no Contrato, o Google notificará o Cliente caso, na opinião do Google, não seja possível cumprir as obrigações nos termos da CCPA, salvo se tal aviso for proibido pela legislação aplicável.

4. Intervenção do Cliente. Se o Google informar ao Cliente sobre o uso não autorizado dos Dados Pessoais do Cliente, incluindo nos termos da Seção 3 (Conformidade) desta subseção ou da Seção 7.2.1 (Notificação de Incidentes), o Cliente poderá tomar as medidas apropriadas e razoáveis para interromper ou corrigir tal uso não autorizado por meio das seguintes ações:

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 Cliente) ou 9.1 (Acesso; Retificação; Tratamento Restrito; Portabilidade).

Turquia

1. Definições Adicionais.

- *Lei Turca de Proteção de Dados* se refere 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* se refere à Kişisel Verileri Koruma Kurumu.
- *SCCs turcas* se refere 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 faturamento do Cliente estiver localizado na Turquia e o Google disponibilizar ao Cliente para aceite termos adicionais opcionais (incluindo SCCs da Turquia) em relação às transferências de Dados Pessoais do Cliente que estão sujeitas à Lei de Proteção de Dados da Turquia, tais termos complementarão este Aditivo a partir da data do recebimento da notificação da Autoridade Turca de Proteção de Dados Pessoais, nos termos da Seção 2.2 (Notificação à Autoridade Competente) abaixo, mediante comprovação apresentada pelo Cliente ao Google.

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

2.3 *Auditorias de SCC*. Se o Cliente 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 Cliente) 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 Cliente concluir, com base em seu uso atual ou planejado dos Serviços, que não estão sendo fornecidas salvaguardas adequadas para os Dados Pessoais do Cliente transferidos, o Cliente 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.

2.5 *Não Modificação de 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 Cliente) 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 regulamentações promulgadas nos termos dessa lei.

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

3. Direitos de Auditoria do Cliente. O Google permitirá que o Cliente ou um auditor independente nomeado pelo Cliente realizem auditorias (incluindo inspeções), nos termos da Seção 7.5.2(a) (Auditoria do Cliente).

Brasil

1.Definições Adicionais.

- "País Adequado" significa, para dados tratados sujeitos à LGPD, o Brasil ou um país ou organização internacional reconhecido pela Autoridade Brasileira de Proteção de Dados (ANPD) como garantidor de proteção adequada nos termos da LGPD.
- "Solução Alternativa de Transferência" significa, para os fins destes termos brasileiros, uma solução, diferente das SCCs do Brasil, que permite a transferência internacional legal de dados pessoais em conformidade com a LGPD.
- "SCCs do Brasil" significa as SCCs do Brasil (Controlador para Operador), as SCCs do Brasil (Operador para Operador) ou as SCCs do Brasil (Operador para Operador, Exportador Google), conforme aplicável.
- "SCCs do Brasil (Controlador para Operador)" significa os termos em https://cloud.google.com/sccs/br-c2p?hl=pt-brXXXX.
- "SCCs do Brasil (Operador para Operador)" significa os termos em https://cloud.google.com/sccs/br-p2p?hl=pt-brXXXX.
- "SCCs do Brasil (Operador para Operador, Exportador Google)" 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 Instruções. Sem prejuízo das obrigações do Google nos termos da Seção 5.2 (Conformidade com as Instruções do Cliente) ou de quaisquer outros direitos ou obrigações de qualquer uma das partes nos termos do Contrato aplicável, o Google notificará imediatamente o Cliente 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 não puder, de outra forma, cumprir uma Instrução, em cada caso, a menos que tal notificação seja proibida pela legislação brasileira.

Se o Cliente for um processador, o Cliente encaminhará imediatamente ao terceiro controlador qualquer notificação fornecida pelo Google nos termos desta seção.

3. Transferências de Dados.

3.1. Transferências Restritas. As partes reconhecem que a LGPD não exige SCCs do Brasil ou uma Solução Alternativa de Transferência para que os Dados Pessoais do Cliente sejam processados ou transferidos para um País Adequado. Se os Dados Pessoais do Cliente 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 Alternativa de Transferência para quaisquer Transferências Restritas BR, o Google informará o Cliente sobre a solução relevante e garantirá que tais Transferências Restritas sejam feitas de acordo com ela; ou

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

i. se o endereço do Google estiver em um País Adequado, as SCCs do Brasil (Operador para Operador, Exportador Google) serão aplicadas em relação a tais Transferências Restritas do Google para Subprocessadores; ou

ii. se o endereço do Google não estiver em um País Adequado, as SCCs do Brasil (Controlador para Operador) ou as SCCs do Brasil (Operador para Operador) serão aplicadas (conforme o Cliente seja um Controlador ou Operador) em relação a tais Transferências Restritas entre o Google e o Cliente.

3.2. Informações sobre Transferências Restritas. O Google fornecerá ao Cliente informações relevantes para as 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. SCCs e Terceiros Controladores. Se o Cliente for um Operador, o Cliente reconhece que o Google, como outro Operador, pode não ser capaz de identificar o terceiro Controlador e, consequentemente, o Cliente irá:

a. encaminhar ao terceiro controlador prontamente e sem atrasos indevidos qualquer notificação referente a quaisquer SCCs do Brasil;

b. ser o único responsável, entre o Google e o Cliente, por garantir a conformidade do terceiro controlador com as obrigações de transparência previstas nas SCCs do Brasil; e

c. mediante solicitação por escrito do Google, fornecer prontamente as seguintes informações sobre o terceiro controlador: nome, dados corporativos (por exemplo, tipo de entidade, endereço registrado, número de identificação fiscal), endereço principal, endereço de email, ponto de contato do titular dos dados e quaisquer detalhes exigidos pelas SCCs do Brasil em relação aos contratos do Clientes com o Controlador.

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

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

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

Apêndice 4: Produtos Específicos

Os termos em cada subseção do Apêndice 4 aplicam-se unicamente ao tratamento dos Dados do Cliente pelo(s) Serviço(s) correspondente(s).

Google Cloud Platform

1. Definições Adicionais.

- *Conta*, caso não seja definido no Contrato, refere-se à conta do Cliente no Google Cloud Platform.
- *Dados do Cliente*, caso não seja definido no Contrato, refere-se aos dados fornecidos ao Google pelo Cliente ou pelos Usuários Finais por meio do Google Cloud Platform usando a Conta, bem como aos dados que o Cliente ou os Usuários Finais derivarem desses dados por meio do uso do Google Cloud Platform.
- *Google Cloud Platform* refere-se aos serviços do Google Cloud Platform descritos em https://cloud.google.com/terms/services, excluindo Produtos de Terceiros.

- *Produtos 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) produtos 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 de Data Centers. Os locais dos data centers do Google Cloud Platform estão 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 estão 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 Adicionais de Segurança e outras medidas de proteção suplementares estão disponíveis em 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. Alterações. Este Aditivo tem as seguintes alterações em relação à Solução Bare Metal:

- A definição de "Auditor Externo do Google" será substituída pelo seguinte:
    - *Auditor Externo do Google* refere-se a um auditor externo independente qualificado, nomeado pelo Google ou por um Subprocessador da Solução Bare Metal, cuja identidade atual o Google informará ao Cliente mediante solicitação.
- Os seguintes termos são excluídos:
    - Na Seção 7.1.1 (Medidas de Segurança do Google), os termos "Criptografar os Dados do Cliente".
    - 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 um ambiente multilocatário em servidores pertencentes a ele. De acordo com as instruções do Cliente em contrário (por exemplo, na forma de uma seleção de local de dados), o Google replica os Dados do Cliente 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 SOC do BMS*).

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

4. Obrigações do Cliente. Sem limitar as obrigações expressas do Google em relação à Solução Bare Metal, o Cliente adotará medidas adequadas para proteger e manter a segurança dos Dados do Cliente e de outros conteúdos armazenados em ou tratados com a 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. Geração de registros 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 Cliente 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 Cliente, software e aplicativos que o Cliente 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. Alterações. A seguinte alteração é feita ao Aditivo em relação ao CNE:

- As Seções 6.1 (Exclusão pelo Cliente) 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 Cliente.

Google Distributed Cloud conectado (Google Cloud Platform)

O Google Distributed Cloud conectado não é implantado em data centers do Google e tem certas características distintas desde a concepção.

1. Alterações. Este aditivo tem as seguintes alterações em relação ao Google Distributed Cloud conectado:

- A definição de **"Incidente de Dados"** é substituída pela seguinte:
    - **"Incidente de Dados"** significa uma violação da segurança do Google que leve à destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilícito a **Dados do Cliente** em sistemas gerenciados ou de outra forma controlados pelo Google, mas para maior clareza, excluindo quaisquer violações que estejam conectadas a hardware ou infraestrutura que sejam gerenciados, hospedados ou operados por, ou de outra forma de responsabilidade do, Cliente.

- 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 Cliente instruirá o Google a excluir todos os Dados do Cliente restantes (incluindo cópias) do Equipamento ao final da Vigência, de acordo com a legislação aplicável. Se quiser reter Dados do Cliente após o final da Vigência, o Cliente deverá exportar ou copiar tais dados antes do final 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 Legislação 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 Cliente".

- 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 Cliente serão armazenados exclusivamente no Equipamento a ser implantado no Local do Cliente.

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 na prestação do Google Distributed Cloud conectado e aprimorar os produtos de segurança nos ambientes de produção do Google Distributed Cloud conectado.

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 de Diffie-Hellman por meio de curvas elípticas efêmeras, assinadas com criptografia 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 conectado tem uma integração CMEK. Consulte mais informações em https://cloud.google.com/kms/docs/cmek.

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

Armazenamento Vinculado. O armazenamento de dados do Cliente 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 conectado.

Multicloud Gerenciado pelo Google (Google Cloud Platform)

Os Serviços Multicloud Gerenciados pelo Google envolvem infraestrutura terceirizada e têm certas características distintas desde a concepção.

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 altera 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 VMware do Cliente ou não possa criptografar os dados pessoais no ambiente VMware do Cliente.

NetApp Volumes (Google Cloud Platform)

1. Alterações. Este Aditivo tem as seguintes alterações em relação a NetApp Volumes:

- A definição de "Auditor Externo do Google" será substituída pelo seguinte:
    - *Auditor Externo do Google* refere-se a um auditor externo independente, nomeado pelo Google ou por um Subprocessador de NetApp Volumes, cuja identidade atual o Google informará ao Cliente 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 Cliente entre data centers dispersos geograficamente. O Google também faz o isolamento lógico dos Dados do Cliente. O Cliente receberá o controle sobre políticas específicas de compartilhamento de dados pessoais. Essas políticas, em conformidade com a funcionalidade dos Serviços, permitirão ao Cliente determinar as configurações de compartilhamento de produtos aplicáveis aos Usuários Finais do Cliente para finalidades específicas. O Cliente 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 SOC do NetApp*).

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

Google Workspace e Cloud Identity

1. Definições Adicionais.

- *Conta*, caso não seja definido no Contrato, refere-se à conta do Cliente no Google Workspace ou no Cloud Identity.
- *Cloud Identity*, quando comprado com um Contrato separado e não como parte do Google Cloud Platform ou do Google Workspace, refere-se aos Serviços do Cloud Identity descritos em https://cloud.google.com/terms/identity/user-features.
- *Dados do Cliente*, caso não seja definido no Contrato, refere-se a dados enviados, armazenados ou recebidos por ou em nome do Cliente ou de seus Usuários Finais por meio do Google Workspace ou do Cloud Identity, usando a Conta.
- *Google Workspace* refere-se aos serviços Google Workspace ou Google Workspace for Education descritos em https://workspace.google.com/terms/user_features.html, conforme aplicável.

2. Produtos Adicionais. Caso o Google, a seu critério, disponibilizar Produtos Adicionais para uso do Cliente com o Google Workspace ou o Cloud Identity, de acordo com o disposto nos Termos dos Produtos Adicionais:

a. O Cliente poderá ativar ou desativar os Produtos Adicionais no Admin Console e não precisará usar os Produtos Adicionais para usar o Google Workspace ou o Cloud Identity.

b. Se o Cliente optar por instalar algum Produto Adicional ou usá-lo com o Google Workspace ou o Cloud Identity, o Produto Adicional poderá acessar os Dados do Cliente, caso necessário, para funcionar com o Google Workspace ou o Cloud Identity, conforme o caso.

Para fins de esclarecimento, o presente Aditivo não se aplica ao tratamento de dados pessoais devido ao provisionamento de Produtos Adicionais instalados ou usados pelo Cliente, incluindo dados pessoais transmitidos por ou para tais Produtos Adicionais.

3. Certificações de Conformidade. As Certificações de Conformidade dos Serviços Auditados do Google Workspace e do Cloud Identity também incluirão certificados ISO 27017 e ISO 27018.

4. Locais de Data Centers. Os locais dos data centers do Google Workspace e do Cloud Identity estão descritos em https://www.google.com/about/datacenters/locations/.

5. Informações sobre Subprocessadores. Os nomes, os locais e as atividades dos Subprocessadores do Google Workspace e do Cloud Identity estão descritos em https://workspace.google.com/intl/en/terms/subprocessors.html.

6. Equipe de Proteção de Dados do Cloud. É possível entrar em contato com a Equipe de Proteção de Dados do Google Workspace e do Cloud Identity (enquanto os Administradores estão conectados à Conta de Administrador) em https://support.google.com/a/contact/googlecloud_dpr.

7. Medidas de Segurança Adicionais. Para o Google Workspace e o Cloud Identity:

a. O Google realiza a separação lógica entre os dados de cada Usuário Final e os dados de outros Usuários Finais.

b. Os dados de um Usuário Final autenticado não serão exibidos para outro Usuário Final, a menos que o primeiro Usuário Final ou um Administrador permita o compartilhamento dos dados.

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

9. Aditivo sobre Dados de Serviço. Se o Google disponibilizar um Aditivo de Dados de Serviço opcional para aceite pelo Cliente em relação ao presente Aditivo, a disponibilidade do aditivo opcional constituirá uma "Atualização de DPA", caso tal termo seja definido em algum Aditivo de Dados de Serviço previamente celebrado pelo Cliente.

10. Termos Específicos de Serviços.

AppSheet (Google Workspace)

1. Alterações. Este Aditivo tem as seguintes alterações em relação ao AppSheet:

- Substitui-se o parágrafo intitulado "Sistemas Operacionais do Servidor", na Seção 1(a) do Apêndice 2 (Medidas de Segurança), pelo seguinte texto:

    - *Sistemas Operacionais do Servidor.* Os servidores do Google usam uma implementação baseada em Linux personalizada para o ambiente do aplicativo.

2. Locais Adicionais de Data Center. Os locais adicionais de data centers do AppSheet estão descritos em https://cloud.google.com/about/locations/.

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 fontes de dados, disponibilizadas pelo Google ao Cliente 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 Cliente 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. Alterações. Este Aditivo tem as seguintes alterações em relação ao Looker (original):

- Substitui-se a definição de "Endereço de E-mail para Notificação" pelo seguinte texto:

    - "Endereço de E-mail para Notificação" refere-se aos endereços de e-mail designados pelo Cliente 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 quaisquer Provedores Terceirizados de Serviço Multicloud tenham instalações".

3. Responsabilidades Adicionais do Cliente sobre Segurança. O Cliente é responsável pela segurança do ambiente, dos bancos de dados e da configuração do Cliente no Looker (original), exceto 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 de Data Centers. Os locais dos data centers do Looker (original) serão descritos no Formulário de Pedido aplicável ou identificados de outra forma pelo Google.

6. Sem Certificação para Clientes Fora da EMEA. O Cliente não tem a obrigação de certificar ou identificar a Autoridade Supervisora competente, nos termos da Seção 4.2 (Certificação por Clientes 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 Adicionais de Segurança 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) estão 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 desde a concepção.

9.1 *Termos de Tratamento de Dados do Multicloud*. O Aditivo sobre Tratamento de Dados do MCS Gerenciado pelo Google complementa e altera 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 Cliente, o Cliente 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 Cliente forneça e atualize tais informações por outros meios.

12. Medidas de Segurança Adicionais para Aplicativos. 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 cliente controlam o acesso dos funcionários do Google aos aplicativos para prestar o suporte técnico solicitado pelo Cliente ou pelos Usuários Finais.

Serviços de SecOps

1. Definições Adicionais.

- *Conta*, caso não seja definido no Contrato, refere-se à conta do Cliente nos Serviços de SecOps ou no Google Cloud Platform, conforme aplicável.

- *Dados do Cliente*, caso não seja definido no Contrato, refere-se (i) a dados fornecidos ao Google pelo Cliente ou pelos Usuários Finais por meio dos Serviços de SecOps usando a Conta e dados que o Cliente ou Usuários Finais derivam desses dados por meio do uso dos Serviços SecOps, ou, (ii) no caso de Serviços de Consultoria da Mandiant e Serviços Gerenciados, dados fornecidos ao Google por Clientes ou usuários finais em conexão com o recebimento de Serviços de SecOps.

- *Provedor Contratado pelo Cliente* refere-se a um provedor de serviço (que pode incluir um operador ou um subprocessador) contratado diretamente pelo Cliente, com um contrato separado entre o Cliente e o provedor.

- *Serviços de SecOps* refere-se aos Serviços de SecOps descritos em https://cloud.google.com/terms/secops/services, excluindo eventuais Produtos de Terceiros.

- *Produtos 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. Alterações. Este Aditivo tem as seguintes alterações em relação aos Serviços de SecOps:

- Substitui-se a definição de "Controles Adicionais de Segurança" pelo seguinte texto:

    - *Controles Adicionais de Segurança* refere-se a recursos, funcionalidades e/ou controles de segurança que o Cliente 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 Operador)" refere-se aos termos disponíveis em: https://cloud.google.com/terms/secops/sccs/eu-c2p.

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

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

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

- A Seção 6.1 (Exclusão pelo Cliente) passará a ter o seguinte texto:

    - 6.1 **Exclusão pelo Cliente**. O Google permitirá que o Cliente exclua os Dados do Cliente durante a Vigência, de maneira consistente com a funcionalidade dos Serviços ou mediante solicitação. Se o Cliente usar os Serviços para excluir Dados do Cliente durante a Vigência e não conseguir recuperar os Dados, ou se o Cliente solicitar a exclusão de Dados do Cliente durante a Vigência, esse uso ou solicitação (conforme o caso) constituirá uma instrução para o Google excluir os Dados do Cliente pertinentes dos sistemas do Google, nos termos da lei aplicável. 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 Legislação Europeia de Proteção de Dados) ou se a legislação relevante exigir a retenção (quando outra Lei de Privacidade Aplicável for pertinente).

- A Seção 9.1 (Acesso, Retificação, Tratamento Restrito e Portabilidade) passará a ter o seguinte texto:

9.1 **Acesso, Retificação, Tratamento Restrito e Portabilidade.** Durante a Vigência, o Google permitirá que o Cliente, de maneira consistente com a funcionalidade dos Serviços, acesse, corrija e restrinja o tratamento dos Dados do Cliente, inclusive nos termos da Seção 6.1 (Exclusão pelo Cliente), e exporte Dados do Cliente mediante solicitação. Se o Cliente tiver conhecimento de que os Dados Pessoais do Cliente estão incorretos ou desatualizados, o Cliente será responsável por notificar o Google, que auxiliará o Cliente na correção dos dados, caso exigido pela Lei de Privacidade Aplicável.

3. Locais de Data Centers. Os locais dos data centers de Serviços de SecOps estão descritos em *https://www.google.com/about/datacenters/locations/*

4. Sem Certificação para Clientes Fora da EMEA. O Cliente não tem a obrigação de certificar ou identificar sua Autoridade Supervisora competente, nos termos da Seção 4.2 (Certificação por Clientes 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://cloud.google.com/terms/secops/subprocessors.

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 Cliente, o Cliente 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 Cliente forneça e atualize tais informações por outros meios.

8. Termos Específicos de Serviços.

Serviços de Consultoria da Mandiant e Serviços Gerenciados

Os Serviços de Consultoria da Mandiant e os Serviços Gerenciados são serviços de consultoria e implementação (incluindo resposta a incidentes, preparação estratégica e garantia técnica para reduzir ameaças e os riscos relacionados a incidentes), bem como serviços gerenciados de detecção e resposta, e tem certas características distintas propositadamente.

1. Alterações. As seguintes alterações são feitas ao Aditivo unicamente com relação aos Serviços de Consultoria da Mandiant e Serviços Gerenciados:

- Complementa-se a definição de "Incidente de Dados" com o seguinte texto:
    - Para fins de esclarecimento, Incidente de Dados exclui os Incidentes que sejam tema dos Serviços de Consultoria da Mandiant e/ou dos Serviços Gerenciados, conforme o caso.
- Substitui-se a Seção 5.2(b)(i) (Conformidade com as Instruções do Cliente) pelo seguinte texto:
    - i. O uso dos Serviços por parte do Cliente.
- A segunda frase da Seção 7.1.1 (Medidas de Segurança do Google) passa a ter o seguinte texto:
    - As Medidas de Segurança poderão incluir (conforme o caso) medidas para criptografar os Dados do Cliente; para manter a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços do Google; para restaurar o acesso rápido aos Dados do Cliente após um incidente; e para fins de testes regulares e eficácia.
- A Seção 7.3.1(b) passa a ter o seguinte texto:
    - b. Cuidar da administração, do acesso e da segurança das credenciais de autenticação da conta, sistemas, software, redes e dispositivos que o Cliente usa para receber, ou autoriza o Google a acessar para prestar os Serviços de Consultoria da Mandiant e/ou os Serviços Gerenciados, conforme o caso.
- Adicionam-se as novas Seções 7.3.1(d) e (e):
    - d. Minimizar a quantidade de Dados do Cliente fornecidos ao Google pelo Cliente ou em nome do Cliente.
    - e. Na medida em que o acesso do Google aos Dados do Cliente esteja sob o controle do Cliente, revogar o acesso quando o Google concluir os Serviços de Consultoria da Mandiant e/ou os Serviços Gerenciados, conforme o caso.
- Substitui-se o Apêndice 2 (Medidas de Segurança) pelo seguinte texto:
    - Apêndice 2: Medidas Técnicas e Organizacionais Adicionais

1. Ambiente Controlado pelo Cliente. O Google apenas acessará e tratará os Dados do Cliente fornecidos ao Google pelo Cliente ou em nome do Cliente por meio de uma conta ou um ambiente controlado ou aprovado pelo Cliente.

2. Políticas e Processos de Acesso a Dados — Política de Acesso. Os processos e políticas de acesso a dados do Google são projetados para evitar que pessoas e/ou sistemas não autorizados consigam acesso a sistemas usados para tratar os Dados do Cliente. O Google: (i) apenas permite que pessoas acessem os dados que elas têm autorização para acessar; (ii) adota medidas para impedir a leitura, a cópia, a alteração ou a remoção de dados pessoais sem autorização durante o tratamento e o uso. A concessão ou a modificação dos direitos de acesso por parte do Google depende de o Cliente provisionar ao Google acesso de usuário final à conta ou ao ambiente do Cliente.

3. Segurança da Equipe. 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 adequadas de histórico para contratação, 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. É necessário que os funcionários que lidam com dados do cliente preencham requisitos adicionais apropriados à sua função (por exemplo, certificações). A equipe do Google não tratará os Dados do Cliente sem autorização.

4. Medidas de Segurança Adicionais. O Google e o Cliente poderão estabelecer por acordo outras medidas de segurança no Formulário de Pedido aplicável, incluindo a eventual ordem de serviço, para os Serviços de Consultoria da Mandiant e/ou os Serviços Gerenciados, conforme aplicável.

2. Provedor Contratado pelo Cliente. Para fins de esclarecimento e sem limitação das obrigações do Google estabelecidas na Seção 7 (Segurança de Dados) ou 11 (Subprocessadores), o Apêndice 2 (Medidas de Segurança) não estabelece as medidas de segurança nem os controles implementados ou fornecidos pelo Cliente ou por Provedores Contratados pelo Cliente.

Serviços de Implementação

1. Definições Adicionais.

- *Dados do Cliente* refere-se aos Dados que o Cliente autoriza a Equipe do Google a acessar nos Sistemas Gerenciados pelo Cliente.

- *Sistemas Gerenciados pelo Cliente* refere-se aos seguintes itens usados pelo Cliente para receber os Serviços de Implementação: (a) instâncias gerenciadas pelo Cliente de Serviços do Google Cloud ou de serviços de nuvem terceirizados; e (b) hardwares ou softwares hospedados ou gerenciados no ambiente local do Cliente.

- *Serviços do Google Cloud* refere-se aos Serviços descritos neste Apêndice 4 (Produtos Específicos), exceto os Serviços de Implementação, os Serviços de Consultoria da Mandiant e os Serviços Gerenciados da Mandiant.

- *Pessoal do Google* refere-se a funcionários e prestadores de serviço do Google envolvidos na prestação dos Serviços de Implementação.

- *Serviços de Implementação* refere-se a serviços de consultoria e implementação prestados por funcionários e prestadores de serviço do Google em suporte aos Serviços do Google Cloud, de acordo com a descrição do Contrato, incluindo em um Formulário de Pedido ou uma Ordem de Serviço.

2. Alterações. Este Aditivo tem as seguintes alterações em relação aos Serviços de Implementação:

- Exclui-se a definição de "Controles Adicionais de Segurança".

- Substitui-se a definição de "Incidente de Dados" pelo seguinte texto:

    - *Incidente de Dados* refere-se a uma violação da Seção 7.1 (Medidas, Controles e Assistência de Segurança do Google) pela Equipe do Google que leve a casos acidentais ou ilegais de destruição, perda, alteração, divulgação não autorizada ou acesso dos Dados Pessoais do Cliente.

- Sujeito ao restante desta seção, o termo "Dados do Cliente" será substituído por "Dados Pessoais do Cliente" quando for usado (a) na Seção 2 (Definições), na definição de "Subprocessador" e (b) em outras seções deste Aditivo. Para fins de esclarecimento, as demais definições da Seção 2 (Definições) permanecerão inalteradas.

- Substitui-se a Seção 3 (Duração) pelo seguinte texto:

    - **3. Duração**. Não obstante a rescisão ou a expiração do Contrato aplicável, este Aditivo permanecerá em vigor até que o Google não tenha mais acesso aos Dados Pessoais do Cliente, ocasião em que o Aditivo expirará automaticamente.

- Substitui-se a Seção 6 (Exclusão de Dados) pelo seguinte texto:

    - **6. Exclusão de Dados.** Ao final da Vigência, o Cliente (a) optará por excluir ou não os Dados Pessoais do Cliente e (b) será responsável por tal exclusão.

- Substitui-se a segunda frase da Seção 7.1.1 (Medidas de Segurança do Google) pelo seguinte texto:

    - "As Medidas de Segurança poderão incluir (conforme o caso) medidas para criptografar os Dados do Cliente; para manter a confidencialidade, a integridade, a disponibilidade e a resiliência contínuas dos sistemas e serviços do Google; para restaurar o acesso rápido aos Dados do Cliente após um incidente; e para fins de testes regulares e eficácia."

- Exclui-se a Seção 7.1.3 (Controles Adicionais de Segurança) e todas as demais referências à seção.

- Substitui-se a Seção 9.1 (Acesso, Retificação, Tratamento Restrito e Portabilidade) pelo seguinte texto:

    - 9.1 *Acesso, Retificação, Tratamento Restrito e Portabilidade*. O Cliente será responsável por usar a funcionalidade dos Sistemas Gerenciados pelo Cliente para acessar e retificar os Dados Pessoais do Cliente e restringir o tratamento de tais dados, incluindo situações em que o Cliente tiver conhecimento de que os Dados Pessoais do Cliente estejam incorretos ou desatualizados e seja necessário, em cumprimento à Lei de Privacidade Aplicável, retificar ou excluir os dados.

- Substitui-se a Seção 11.4 (Direito de Oposição a Subprocessadores) pelo seguinte texto:

    - 11.4 *Direito de Oposição a Subprocessadores*. Quando houver a contratação de um Novo Subprocessador durante a Vigência, o Google informará ao Cliente sobre a contratação do Novo Subprocessador antes que este processe os Dados Pessoais do Cliente. O Cliente poderá apresentar uma objeção ao Novo Subprocessador enviando uma notificação ao Google, caso em que as partes trabalharão de boa fé para encontrar uma alternativa mutuamente aceitável.

- O Apêndice 1 (Objeto em Questão e Detalhes do Tratamento de Dados) passa a ter este texto:

    - Substitui-se a seção "Duração do Tratamento" pelo seguinte texto:

        - *Duração do Tratamento*. A Vigência mais o período do final da Vigência até a expiração do acesso do Google aos Dados Pessoais do Cliente (se aplicável).

    - Substituem-se as palavras "fornecidos ao Google por meio dos Serviços", nas seções "Categorias de Dados" e "Titulares de Dados", por "disponibilizados ao Google em conexão com os Serviços".

- Substitui-se o Apêndice 2 (Medidas de Segurança) pelo seguinte texto:

    - **Apêndice 2: Medidas de Segurança**

1. Sistemas Gerenciados pelo Cliente. O Pessoal do Google apenas acessará e processará os Dados Pessoais do Cliente nos Sistemas Gerenciados pelo Cliente. Se esses sistemas incluírem Serviços do Google Cloud, o uso dos Serviços do Google Cloud por parte do Cliente continuará sujeito ao contrato aplicável a esses serviços.

2. Controle de Acesso. As políticas e os processos internos de acesso a dados do Google são criados para evitar que pessoas e sistemas não autorizados tenham acesso aos Serviços do Google Cloud usados para tratar os dados pessoais. As políticas do Google (i) permitem que a Equipe do Google acesse apenas os dados que eles têm autorização para acessar e (ii) requerem que a Equipe do Google não leia, copie, altere nem remova os Dados Pessoais do Cliente sem autorização durante o tratamento e o uso e após a gravação. O Cliente controla o provisionamento ou a modificação dos direitos dos usuários finais de acessar os Sistemas Gerenciados pelo Cliente. Caso esses sistemas incluam Serviços do Google Cloud, detalhes sobre ferramentas de fluxo que trabalho que mantêm

registros de auditoria de mudanças e registros de acesso ao sistema estão disponíveis no contrato dos Serviços do Google Cloud aplicável.

3. Segurança da Equipe. 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 adequadas de histórico para contratação, dentro do legalmente permitido e de acordo com as leis trabalhistas locais e regulamentações estatutárias aplicáveis.

A Equipe do Google 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 do Google recebe treinamento de segurança. A Equipe do Google que lida com Dados Pessoais do Cliente precisa satisfazer outros requisitos adequados à respectiva função (por exemplo, certificações).

4. Medidas de Segurança Adicionais. O Google e o Cliente poderão estabelecer, de comum acordo, outras medidas de segurança no Contrato, incluindo em um Formulário de Pedido ou uma Ordem de Serviço.

5. Segurança do Subprocessador. Antes da integração de Subprocessadores, 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.

3. Responsabilidades de Segurança do Cliente. Além das obrigações estabelecidas na Seção 7.3.1 (Responsabilidades de Segurança do Cliente), o Cliente é responsável pelo seguinte:

- Cuidar da administração, do acesso e da proteção dos Sistemas Gerenciados pelo Cliente, incluindo minimizar o acesso da Equipe do Google aos Dados Pessoais do Cliente na medida em que seja viável, bem como encerrar o acesso mediante a conclusão dos Serviços de Implementação.

- Implementar eventuais recomendações de segurança que o Google venha a fornecer por escrito ao Cliente em relação aos Sistemas Gerenciados pelo Cliente.

4. Certificação de Conformidade. O Google manterá os certificados ISO 27001, ISO 27017 e ISO 27018, que abrangem os Serviços de Implementação prestados em suporte ao Google Cloud Platform e ao Google Workspace (*Certificações de Conformidade dos Serviços de Implementação*). O Google poderá adicionar padrões a qualquer momento. O Google poderá substituir uma Certificação de Conformidade de Serviços de Implementação por uma alternativa equivalente ou aprimorada.

5. Revisões de Certificado de Conformidade. Para demonstrar a conformidade com suas obrigações estabelecidas pelo Aditivo, o Google disponibilizará a Certificação de Conformidade dos Serviços de Implementação para análise do Cliente e, caso o Cliente seja operador, permitirá que o Cliente solicite, para o terceiro controlador, o acesso à Certificação de Conformidade dos Serviços de Implementação.

6. Locais de Tratamento de Dados. Os Dados Pessoais do Cliente poderão ser tratados em qualquer país onde o Google preste os serviços de Implementação ou onde o Cliente mantiver Sistemas Gerenciados pelo Cliente.

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

8. Informações sobre Subprocessadores. Os Subprocessadores dos Serviços de Implementação serão identificados (como subprestadores de serviços) em um Formulário de Pedido ou Ordem de Serviço relevante ou em outra confirmação enviada ao Cliente antes do início dos Serviços de Implementação ou serão Afiliados do Google. O Google também disponibilizará ao Cliente, mediante solicitação, os nomes, os locais e as atividades dos Subprocessadores dos Serviços de Implementação.

9. 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 Cliente, o Cliente 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 Cliente forneça e atualize tais informações por outros meios.

Google Cloud Skills Boost para Organizações

1. Definições Adicionais.

- *Conta*, caso não seja definido no Contrato, significa a Conta do Cliente no Google Cloud Skills Boost para Organizações.
- *GCSBO* refere-se a serviços e conteúdo educacionais, de treinamento e de aprendizado oferecidos por https://www.cloudskillsboost.google/ (ou outro site operado e controlado pelo Google e usado para fins do Google Cloud Skills Boost para Organizações).
- *SST* refere-se aos serviços de suporte técnico que o Google poderá, a seu critério, prestar ao Cliente.

2. Alterações. Este Aditivo tem as seguintes alterações em relação ao GCSBO:

- Substitui-se a definição de "Controles Adicionais de Segurança" pelo seguinte texto:
    - *Controles Adicionais de Segurança* refere-se a recursos, funcionalidades e/ou controles de segurança que o Cliente 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 Operador)" refere-se aos termos disponíveis em: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-c2p.
- "SCCs (Operador para Controlador)" refere-se aos termos disponíveis em: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2c.
- "SCCs (Operador para Operador)" refere-se aos termos disponíveis em: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p.
- SCCs (Operador para Operador, Exportador do Google) refere-se aos termos disponíveis em: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p-intra-group.

3. Locais de Data Centers. Os locais dos data centers do GCSBO estão descritos em https://cloud.google.com/about/locations/.

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

5. Informações sobre Subprocessadores. Os nomes, os locais e as atividades dos Subprocessadores do GCSBO estão descritos em:

a. https://cloud.google.com/terms/skillsboost-organizations/subprocessors; and

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

6. Equipe de Proteção de Dados do Cloud. É possível entrar em contato com a Equipe de Proteção de Dados do GCSBO em https://support.google.com/qwiklabs (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 Cliente, o Cliente 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 Cliente forneça e atualize tais informações por outros meios.

Versões anteriores dos Termos de Tratamento e Segurança de Dados:

9 de abril de 2024 30 de junho de 2022 24 de setembro de 2021 19 de agosto de 2020 10 de agosto de 2020 17 de julho de 2020 11 de outubro de 2019 1º de outubro de 2019 25 de maio de 2018 13 de março de 2018 9 de novembro de 2017 11 de outubro de 2017 7 de fevereiro de 2017 6 de outubro de 2016

Versões anteriores do Aditivo sobre Tratamento de Dados:

7 de julho de 2022 *24 de setembro de 2021* *27 de maio de 2021* *29 de outubro de 2019* *25 de maio de 2018* *25 de abril de 2018* *11 de julho de 2017* *28 de novembro de 2016* *7 de janeiro de 2016* *24 de abril de 2015* *1º de abril de 2014* *14 de novembro de 2012*

Versões anteriores do Aditivo sobre Tratamento de Dados para Serviços do Looker (original) (Clientes):

14 de fevereiro de 2023 4 de janeiro de 2023 20 de setembro de 2022 30 de junho de 2022 16 de março de 2022 24 de setembro de 2021 1º de abril de 2021 15 de janeiro de 2021 17 de dezembro de 2020 28 de agosto de 2020 1º de junho de 2020 9 de março de 2020

Versões anteriores de DPST de Serviços de SecOps (Clientes):

6 de fevereiro de 2023 28 de novembro de 2022 27 de setembro de 2021 1º de outubro de 2020

Versões anteriores do Aditivo sobre Tratamento de Dados para Serviços de Consultoria de SecOps e Serviços Gerenciados:

5 de outubro de 2023 19 de setembro de 2023 15 de junho 2023 22 de fevereiro de 2023 6 de fevereiro de 2023

Versões anteriores *(última modificação em 04 de setembro de 2025)*

26 de setembro de 2024 9 de setembro de 2024 5 de agosto de 2024 23 de maio de 2024 9 de abril de 2024 8 de novembro de 2023 15 de agosto de 2023 20 de setembro de 2022