ADENDO DE PROCESSAMENTO DE DADOS DA COMMAND ALKON INCORPORATED

Atualizado: 25/07/24

Este Adendo de Processamento de Dados (" DPA ") faz parte do Contrato *Principal de Licença e Serviços ("* **Contrato ") entre: (i) Cliente (identificado no Contrato Principal de Licença e Serviços) e suas afiliadas do EEE ("Cliente"); e (ii) a Command Alkon Incorporated e suas afiliadas (" Empresa ") somente quando exigido pelo Regulamento Geral de Proteção de Dados ("GDPR") ou outra privacidade aplicável** legislação.

Este Adendo substitui qualquer acordo anterior entre as partes em relação ao assunto aqui tratado, ou seja, privacidade e segurança de dados, conforme aplicável à legislação de privacidade.

Em consideração às obrigações mútuas aqui estabelecidas, as partes concordam que os termos e condições estabelecidos abaixo serão adicionados como um Adendo ao Contrato.

1. Definições

"**Dados pessoais do cliente**" significam dados pessoais processados pela empresa em nome do cliente no fornecimento dos produtos e/ou serviços.

"**CCPA**" significa a Lei de Privacidade do Consumidor da Califórnia, conforme alterada pela Lei de Direitos de Privacidade da Califórnia ou por outra legislação/regulamentação da Califórnia.

"**Titular dos dados**" significa o indivíduo a quem os Dados Pessoais do Cliente se relacionam.

"Estrutura de Privacidade de Dados" significa a estrutura legal UE-EUA para transferências transfronteiriças de Dados Pessoais entre a União Europeia e os Estados Unidos e inclui a extensão do Reino Unido para a UE-EUA O DPF e o Swiss-U.S. PDF.

"**Leis de proteção de dados**" significam todas as leis e regulamentos aplicáveis relacionados ao processamento de dados pessoais e à privacidade que possam existir nas jurisdições relevantes, incluindo, quando aplicável, o Regulamento Geral de Proteção de Dados (UE) 2016/679 sobre a proteção de pessoas físicas em relação ao processamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/EC ("GDPR") (e qualquer alteração ou substituição a ela), o Lei Federal Suíça sobre Proteção de Dados ("FADP") (e qualquer emenda ou substituição a ela), o GDPR da UE, conforme alterado e incorporado à legislação do Reino Unido sob a Lei da União Europeia (Retirada) do Reino Unido de 2018 e a legislação secundária aplicável feita sob essa Lei ("GDPR do Reino Unido") (e qualquer emenda ou substituição a ela), a Lei Canadense de Proteção de Informações Pessoais e Documentos Eletrônicos ("PIPEDA") (e qualquer emenda ou substituição a ela), a Lei Geral de Proteção de Dados do Brasil (a "LGPD") (e qualquer emenda ou substituição a ela)), a Lei de Privacidade de 1988 (Cth) da Austrália, conforme alterada ("Lei de Privacidade Australiana") (e qualquer emenda ou substituição a ela), U.S. leis estaduais de privacidade (incluindo a CCPA e a CPRA da Califórnia), conforme emitidas ou alteradas, ou qualquer

outra legislação de privacidade aplicável que exija um DPA. Quando o GDPR for mencionado especificamente, os mesmos requisitos se aplicarão a qualquer outro requisito equivalente da Lei de Proteção de Dados aplicável.

"**Dados pessoais**" significa qualquer informação relacionada a um titular dos dados, incluindo, mas não se limitando a um nome, um número de identificação, dados de localização, um identificador on-line ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social do titular dos dados.

"**Processo**" ou "**Processamento**" significa qualquer operação ou conjunto de operações realizadas nos Dados Pessoais do Cliente, seja por meios automatizados ou não, como coleta, gravação, organização, estruturação, armazenamento, alteração, recuperação, consulta, uso, divulgação, descarte, restrição, acesso, disseminação, combinação, adaptação, cópia, transferência, exclusão e/ou destruição dos Dados Pessoais do Cliente.

"**Violação de segurança**" significa uma violação confirmada de segurança que leva a uma destruição acidental ou ilegal, perda, alteração, divulgação ou acesso não autorizados aos Dados Pessoais do Cliente transmitidos, armazenados ou processados de outra forma.

"**Cláusulas contratuais padrão**" significam os requisitos contratuais padrão estabelecidos pela Lei de Proteção de Dados aplicável (cláusulas contratuais padrão da UE, cláusulas contratuais modelo do Conselho de Proteção de Dados da RIPD, cláusulas contratuais modelo da ASEAN, etc.).

"Terceiro" significa uma parte que não seja o Cliente ou a Empresa.

Os termos "**controlador**", "**processador**" e "**autoridade supervisora**", conforme usados neste DPA, terão os significados atribuídos a eles na Lei de Proteção de Dados aplicável.

Todos os outros termos não definidos, mas em maiúsculas, terão o significado estabelecido no Contrato ou na Lei de Proteção de Dados aplicável.

2. Processamento de dados pessoais do cliente

2.1 Objetivo do processamento. O objetivo do processamento de dados sob este DPA é o fornecimento dos produtos e/ou serviços de acordo com o Contrato. O Anexo 1 descreve o assunto e os detalhes do processamento de dados pessoais do cliente.

2.2 Responsabilidades do processador e do controlador. As partes reconhecem e concordam que: (a) a Empresa é processadora de Dados Pessoais do Cliente de acordo com as Leis de Proteção de Dados; (b) o Cliente é o controlador dos Dados Pessoais do Cliente de acordo com as Leis de Proteção de Dados; (c) o Cliente é responsável por obter todas as autorizações e aprovações necessárias para inserir, usar, fornecer, armazenar e processar os Dados Pessoais do Cliente para permitir que a Empresa forneça os produtos e/ou serviços; e (d) cada parte cumprirá as obrigações aplicáveis a de acordo com as Leis de Proteção de Dados com relação ao processamento de Dados pessoais do cliente.

2.3 Leis de proteção de dados dos EUA. Para fins das leis de proteção de dados dos EUA (incluindo a CCPA), "controlador" inclui "empresa"; "processador" inclui "provedor

de serviços"; "Titular dos dados" inclui "consumidor"; e "Dados pessoais" inclui "informações pessoais". A empresa é uma prestadora de serviços e o cliente é uma empresa.

2.4 Instruções para o cliente. O Cliente instrui a Empresa a processar os Dados Pessoais do Cliente: (a) de acordo com o Contrato e qualquer Suplemento aplicável; (b) conforme necessário para fornecer os produtos e/ou serviços ao Cliente; (c) conforme necessário para cumprir a lei ou regulamentação aplicável; e (d) para cumprir outras instruções escritas razoáveis fornecidas pelo Cliente, quando tais instruções forem consistentes com os termos do Contrato. O Cliente garantirá que suas instruções para o Processamento de Dados Pessoais do Cliente estejam em conformidade com as Leis de Proteção de Dados. Entre as partes, o Cliente será o único responsável pela precisão, qualidade e legalidade dos Dados Pessoais do Cliente e pelos meios pelos quais o Cliente obteve os Dados Pessoais do Cliente.

2.5 Conformidade da empresa com as instruções do cliente. A Empresa só processará os Dados Pessoais do Cliente de acordo com as instruções do Cliente e tratará os Dados Pessoais do Cliente como informações confidenciais. Se a Empresa acreditar ou tomar conhecimento de que alguma das instruções do Cliente está em conflito com qualquer Lei de Proteção de Dados, a Empresa informará o Cliente dentro de um prazo razoável. A Empresa pode processar os Dados Pessoais do Cliente de forma diferente das instruções escritas do Cliente, se isso for exigido pela lei aplicável à qual a Empresa está sujeita. Nessa situação, a Empresa informará o Cliente sobre tal exigência antes que a Empresa processe os Dados Pessoais do Cliente, a menos que seja proibido pela lei aplicável.

2.6 Processamento CCPA. Na medida em que o processamento de dados pessoais pela empresa está sujeito à CCPA, a empresa certifica que não deve: (a) reter, usar ou divulgar dados pessoais do cliente além dos previstos no Contrato, conforme necessário para fornecer os produtos e/ou serviços, criar ou melhorar a qualidade dos produtos e/ou serviços, detectar incidentes de segurança, proteger contra atividades fraudulentas ou ilegais, reter subprocessadores de acordo com este DPA, ou como de outra forma permitido pela CCPA; ou (b) vender ou compartilhar Dados Pessoais do Cliente.

3. Subprocessadores

3.1 Nomeação de subprocessadores. O Cliente fornece autorização geral por escrito para que a Empresa contrate subprocessadores terceirizados para fornecer serviços limitados ou auxiliares relacionados ao fornecimento de produtos e/ou serviços. O site da Empresa lista os subprocessadores que estão atualmente contratados pela Empresa para realizar atividades de processamento específicas relacionadas aos Dados Pessoais do Cliente (https://commandalkon.com/sub-processor-list/) e a Empresa atualizará a lista de subprocessadores antes de contratar qualquer novo subprocessador para realizar um processamento específico. O cliente pode se inscrever para receber atualizações eletrônicas sempre que a lista de subprocessadores da Empresa for alterada, enviando essa solicitação para privacy@commandalkon.com. O Cliente pode se opor a qualquer subprocessador comunicando tal objeção à Empresa dentro de trinta (30) dias após a atualização, e as partes trabalharão de boa fé para resolver a

objeção. O cliente concorda com as atividades de subprocessamento dos subprocessadores atuais listados no site da Empresa.

3.2 Segurança do subprocessador. Quando a Empresa subcontrata suas obrigações, ela deve fazê-lo somente por meio de um acordo escrito com o subprocessador que impõe obrigações contratuais que sejam pelo menos equivalentes às obrigações impostas à Empresa sob este Adendo. As partes concordam que as cópias dos contratos com subprocessadores autorizados que devem ser fornecidas de acordo com as Cláusulas Contratuais Padrão aplicáveis serão fornecidas somente mediante solicitação por escrito do Cliente.

3.3 Responsabilidade. Quando o subprocessador não cumprir suas obrigações de proteção de dados nos termos desse contrato escrito, a Empresa permanecerá totalmente responsável perante o Cliente pelo desempenho das obrigações do subprocessador nos termos desse contrato.

4. Responsabilidades de segurança

4.1 Segurança da empresa. A Empresa implementará medidas técnicas e organizacionais apropriadas para proteger os Dados Pessoais do Cliente ("**Programa de Segurança da Informação**"), levando em consideração o estado da arte, os custos de implementação e a natureza, escopo, contexto e propósitos do Processamento, bem como o risco de probabilidade e severidade variáveis dos direitos e liberdades das pessoas físicas. A empresa se governa de acordo com os seguintes padrões de segurança: NIST 800-171; AWS CIS.

4.2 Segurança do cliente. O Cliente reconhece que os produtos e/ou serviços incluem certos recursos e funcionalidades que o Cliente pode optar por usar e que afetam a segurança dos Dados Pessoais do Cliente processados pelo uso dos produtos e/ou serviços pelo Cliente. O Cliente é responsável por revisar as informações que a Empresa disponibiliza sobre sua segurança de dados e por determinar de forma independente se os produtos e/ou serviços atendem aos requisitos e obrigações legais do Cliente, incluindo suas obrigações de acordo com a Lei de Proteção de Dados aplicável. O Cliente também é responsável por configurar adequadamente os produtos e/ou serviços e usar os recursos e funcionalidades disponibilizados pela Empresa para manter a segurança adequada à luz da natureza dos Dados Pessoais do Cliente processados como resultado do uso dos produtos e/ou serviços pelo Cliente. O Cliente é responsável pelo uso dos produtos e/ou serviços e pelo armazenamento de quaisquer cópias dos Dados Pessoais do Cliente fora dos sistemas da Empresa ou dos subprocessadores da Empresa, incluindo, mas não se limitando a, proteger as credenciais, sistemas e dispositivos de autenticação da conta e reter cópias dos Dados Pessoais do Cliente, conforme apropriado.

4.3 Pessoal da empresa. A Empresa deve garantir que seu pessoal envolvido no Processamento de Dados Pessoais do Cliente seja informado sobre a natureza confidencial dos Dados Pessoais do Cliente, tenha recebido treinamento apropriado sobre suas responsabilidades e esteja sujeito às obrigações de confidencialidade, com tais obrigações sobrevivendo ao término do contrato desse indivíduo com a Empresa.

4.4 Teste de segurança. A Empresa testará, avaliará e avaliará a eficácia do Programa de Segurança da Informação para garantir o processamento seguro dos Dados Pessoais do Cliente. A Empresa cumprirá seu Programa de Segurança da Informação e declara e garante que seu Programa de Segurança da Informação está e estará em conformidade com a legislação aplicável.

4.5 Avaliações de impacto. A Empresa tomará medidas razoáveis para cooperar e auxiliar o Cliente na realização de avaliações de impacto e consultas relacionadas com qualquer autoridade supervisora se o Cliente for obrigado a realizar tais avaliações de impacto de acordo com as Leis de Proteção de Dados.

5. Direitos do titular dos dados

5.1 Assistência com as obrigações do cliente. Na medida em que o Cliente, ao usar ou receber os produtos e/ou serviços, não tenha a capacidade de corrigir, alterar, restringir, bloquear ou excluir os Dados Pessoais do Cliente conforme exigido pelas Leis de Proteção de Dados, a Empresa cumprirá prontamente as solicitações razoáveis do Cliente para facilitar tais ações na medida em que a Empresa seja legalmente permitida e capaz de fazê-lo. Se legalmente permitido, o Cliente será responsável por qualquer custo decorrente da prestação dessa assistência pela Empresa.

5.2 Obrigações de notificação. A Empresa deverá, na medida do legalmente permitido, notificar imediatamente o Cliente se receber uma solicitação de um Titular de Dados para acesso, correção, alteração, exclusão ou objeção ao Processamento de Dados Pessoais do Cliente relacionados a esse indivíduo. A Empresa não responderá a nenhuma solicitação do Titular dos Dados relacionada aos Dados Pessoais do Cliente sem o consentimento prévio por escrito do Cliente, exceto para confirmar que a solicitação está relacionada ao Cliente. Além disso, a Empresa deverá, na medida do legalmente permitido, notificar imediatamente o Cliente se receber uma solicitação de divulgação ou correspondência, notificação ou outra comunicação relacionada aos Dados Pessoais do Cliente da polícia, de uma autoridade competente ou de uma autoridade de proteção de dados relevante. A Empresa fornecerá ao Cliente cooperação e assistência adequadas e razoáveis em relação ao tratamento de qualquer solicitação desse tipo, na medida legalmente permitida e na medida em que o Cliente não tenha acesso a esses Dados Pessoais do Cliente por meio do uso ou recebimento dos produtos e/ou serviços. Se legalmente permitido, o Cliente será responsável por qualquer custo decorrente da prestação dessa assistência pela Empresa.

6. Violação de dados pessoais

6.1 Obrigações de notificação. Caso a Empresa tome conhecimento de uma Violação de Segurança verificada envolvendo Dados Pessoais do Cliente, a Empresa notificará o Cliente sobre a Violação de Segurança sem demora injustificada e, em qualquer caso, no máximo setenta e duas (72) horas após a confirmação. As obrigações desta Seção 6 não se aplicam a incidentes causados pelo Cliente, pela equipe ou pelos usuários finais do Cliente ou a tentativas ou atividades malsucedidas que não comprometam a segurança dos Dados Pessoais do Cliente, incluindo tentativas malsucedidas de login, pings, escaneamentos de portas, ataques de negação de serviço e outros ataques de rede a firewalls ou sistemas em rede.

6.2 Forma de notificação. A notificação de violações de segurança, se houver, será entregue ao ponto de contato do Cliente por e-mail ou telefone. É responsabilidade exclusiva do Cliente garantir que ele mantenha informações de contato precisas nos sistemas de suporte da Empresa em todos os momentos. O Cliente é o único responsável por cumprir os requisitos de notificação de violação aplicáveis ao Cliente e cumprir quaisquer obrigações de notificação de terceiros relacionadas a qualquer Violação de Segurança de Dados Pessoais.

6.3 Conteúdo da notificação. Sempre que seja necessária uma notificação, essa notificação deve, no mínimo:

6.3.1 descrever a natureza da violação de segurança, as categorias e números de titulares de dados envolvidos e as categorias e números de registros de dados pessoais em questão;

6.3.2 comunicar o nome e os detalhes de contato do contato relevante da Empresa, do qual mais informações podem ser obtidas;

6.3.3 descrever as prováveis consequências da violação de segurança; e

6.3.4 descreva as medidas tomadas ou propostas para resolver a violação de segurança.

7. Exclusão ou devolução de dados pessoais do cliente

7.1 Excluir ou devolver. De acordo com a seção 7.3, a Empresa concorda em, imediatamente e em qualquer caso, dentro de trinta (30) dias a partir da data de cessação de quaisquer serviços que envolvam o processamento de dados pessoais do cliente (a "**Data de cessação**"), excluir com segurança os dados pessoais do cliente ou, mediante solicitação por escrito do cliente, devolver uma cópia completa de todos e quaisquer dados pessoais do cliente ao cliente por meio de transferência segura de arquivos no formato razoavelmente solicitado pelo cliente.

7.2 Se o Cliente e a Empresa tiverem celebrado Cláusulas Contratuais Padrão exigindo a certificação de exclusão por escrito (como as Cláusulas 8.5 e 16 dos SCCs da UE), as partes concordam que a certificação por escrito só será fornecida mediante solicitação por escrito do Cliente.

7.3 Definição de Excluir. Para fins de esclarecimento, "**Excluir**" significa remover ou apagar os Dados Pessoais do Cliente de forma que não possam ser recuperados ou reconstruídos.

7.4 Registros. A Empresa pode reter os Dados Pessoais do Cliente na medida exigida pelas Leis Aplicáveis ou conforme determinado no cronograma de retenção de documentos da Empresa, desde que a Empresa garanta a confidencialidade de todos esses Dados Pessoais do Cliente.

8. Direitos de auditoria

8.1 Direitos de auditoria. No máximo uma vez por ano, o Cliente pode contratar um terceiro mutuamente acordado para auditar a Empresa exclusivamente com o objetivo de atender aos requisitos de auditoria de acordo com o Artigo 28, Seção 3 (h) do GDPR. Para solicitar uma auditoria, o Cliente deve enviar um plano de auditoria detalhado pelo menos quatro (4) semanas antes da data de auditoria proposta, descrevendo o escopo, a duração e a data de início da auditoria propostos. As solicitações de auditoria devem ser enviadas para privacy@commandalkon.com. O auditor deve assinar um acordo de confidencialidade por escrito aceitável para a Empresa antes de conduzir a auditoria. A auditoria deve ser conduzida durante o horário comercial normal, sujeita às políticas da Empresa, e não pode interferir injustificadamente nas atividades comerciais da Empresa. Todas as auditorias são por conta e despesa exclusivas do Cliente. A Empresa cooperará com qualquer solicitação de auditoria do Cliente ou de qualquer autoridade reguladora ou supervisora competente para verificar a conformidade da Empresa com suas obrigações nos termos deste DPA, disponibilizando, sujeitos a obrigações de não divulgação, relatórios de auditoria de terceiros, quando disponíveis, e/ou descrições de controles de segurança e outras informações razoavelmente solicitadas pelo Cliente em relação às práticas e políticas de segurança da Empresa.

8.2 Assistência de conformidade. Levando em consideração a natureza do Processamento e as informações disponíveis para a Empresa, a Empresa fornecerá cooperação e assistência adequadas e razoáveis ao Cliente em relação às obrigações de conformidade do Cliente descritas nos artigos 32-36 do GDPR.

9. Transferências de dados

9.1 Autorização geral. O Cliente concorda que a Empresa pode, de acordo com a Seção 9.2, armazenar e processar Dados Pessoais do Cliente nos Estados Unidos da América e em qualquer outro país no qual a Empresa ou qualquer um de seus subprocessadores mantenha instalações ou processe Dados Pessoais. Quaisquer transferências desse tipo serão regidas primeiro pela certificação da Estrutura de Privacidade de Dados da Empresa ou, alternativamente, pelas Cláusulas Contratuais Padrão interafiliadas da Empresa. A Empresa não transferirá, nem fará com que sejam transferidos, quaisquer Dados Pessoais do Cliente de uma jurisdição para outra, a menos que esteja de acordo com a lei aplicável e não fará com que o Cliente viole nenhuma Lei de Proteção de Dados.

9.2 Cláusulas contratuais padrão. Na medida em que, e somente na medida em que, a Empresa processa os Dados Pessoais do Cliente do Espaço Econômico Europeu e as cláusulas contratuais padrão são necessárias, o Módulo Dois das Cláusulas Contratuais Padrão se aplicará e será incorporado aqui. Para fins das Cláusulas Contratuais Padrão, o Cliente é o "exportador de dados" e a Empresa é a "importadora de dados".

9.3 Adendo do Reino Unido às cláusulas contratuais padrão da UE. Na medida em que, e somente na medida em que, a Empresa processa os Dados Pessoais do Cliente do Reino Unido e as cláusulas contratuais padrão são necessárias, as partes concordam que o Adendo do Reino Unido se aplicará aos Dados Pessoais transferidos por meio

dos produtos e/ou serviços do Reino Unido, diretamente ou por meio de transferência posterior, para qualquer país ou destinatário fora do Reino Unido que não seja reconhecido pela autoridade reguladora competente do Reino Unido ou órgão governamental como fornecendo uma nível de proteção para dados pessoais.

9.4 FADP suíço. Na medida em que, e somente na medida em que a empresa processa dados pessoais de clientes da Suíça, os seguintes requisitos adicionais se aplicam na medida em que as transferências de dados estejam sujeitas exclusivamente ao FADP ou estejam sujeitas ao FADP e ao GDPR da UE: (a) o termo "estado membro" não deve ser interpretado de forma a excluir os titulares de dados na Suíça da possibilidade de processar seus direitos em seu local de residência habitual (Suíça) em de acordo com a Cláusula 18 (c) das Cláusulas Contratuais Padrão; (b) na medida em que as transferências de dados subjacentes às Cláusulas Contratuais Padrão estão sujeitas exclusivamente ao FADP, as referências ao GDPR da UE devem ser entendidas como referências ao FADP; e (c) na medida em que as transferências de dados subjacentes às Cláusulas Contratuais Padrão estejam sujeitas ao FADP e ao GDPR da UE, as referências ao GDPR da UE devem ser entendidas como referências ao FADP, na medida em que as transferências de dados estão sujeitas ao FADP P.

9.5 Medidas complementares. Em complemento às Cláusulas Contratuais Padrão, se a Empresa tomar conhecimento de que alguma autoridade governamental (incluindo a polícia) deseja obter acesso ou uma cópia de alguns ou de todos os Dados Pessoais do Cliente processados pela Empresa, seja de forma voluntária ou obrigatória, para fins relacionados à inteligência de segurança nacional, a menos que seja legalmente proibido ou sob uma compulsão legal obrigatória que exija o contrário, a Empresa: 1) notificará imediatamente o Cliente a quem os Dados Pessoais se aplicam; 2) informará a autoridade governamental relevante que não foi autorizada a divulgar os Dados Pessoais do Cliente e, a menos que seja legalmente proibida, precisará notificar imediatamente o Cliente a quem os Dados Pessoais do Cliente se aplicam; 3) informar à autoridade governamental que ela deve direcionar todas as solicitações ou demandas diretamente ao Cliente a quem os Dados Pessoais do Cliente se aplicam; e 4) não fornecer acesso aos Dados Pessoais do Cliente até que seja autorizada por escrito pelo Cliente a quem os Dados Pessoais do Cliente se aplicam ou até que seja legalmente obrigada a fazê-lo. Se legalmente obrigada a fazê-lo, a Empresa envidará esforços razoáveis e legais para contestar tal proibição ou compulsão. Se a Empresa for obrigada a produzir os Dados Pessoais do Cliente, a Empresa só divulgará os Dados Pessoais do Cliente na medida legalmente exigida, de acordo com o processo legal aplicável.

9.6 Lei de vigilância de inteligência estrangeira. A empresa não recebeu anteriormente nenhuma diretriz sob a Seção 702 da Lei de Vigilância de Inteligência Estrangeira dos EUA, codificada em 50 U.S.C. §1881a ("Seção 702 da FISA"). Nenhum tribunal considerou a Empresa o tipo de entidade elegível para receber o processo emitido de acordo com a Seção 702 da FISA. *A empresa não é o tipo de fornecedor elegível para estar sujeito à coleta a montante (coleta "em massa") de acordo com a Seção 702 da FISA, conforme descrito na decisão Schrems II.*

9.7 Precedência de transferência. Caso os serviços sejam cobertos por mais de um mecanismo de transferência, a transferência dos Dados Pessoais do Cliente estará

sujeita a um único mecanismo de transferência, de acordo com a seguinte ordem de precedência: (i) certificação da Estrutura de Privacidade de Dados da Empresa; (ii) Cláusulas Contratuais Padrão aplicáveis (quando exigidas pela Lei de Proteção de Dados aplicável).

10. Prazo e rescisão

Prazo do DPA. Este DPA entrará em vigor na data em que o Contrato for totalmente executado e, apesar da expiração do prazo de qualquer assinatura adquirida, permanecerá em vigor até a exclusão de todos os Dados Pessoais do Cliente, conforme descrito neste DPA, e expirará automaticamente após a exclusão.

11. Não conformidade; soluções; partes

11.1 Limitação de responsabilidade. A responsabilidade da Empresa pela violação de suas obrigações neste DPA está sujeita à cláusula de limitação de responsabilidade no Contrato.

11.2 Partes deste DPA. Nada no DPA conferirá quaisquer benefícios ou direitos a qualquer pessoa ou entidade que não seja as partes deste DPA.

12. Termos gerais

Lei aplicável e jurisdição

12.1 Esse DPA será revisado um ano a partir da data de emissão e três anos depois, ou antes, se apropriado.

12.2 A menos que exigido pelas Cláusulas Contratuais Padrão:

12.2.1 as partes deste Adendo se submetem à escolha de jurisdição estipulada no Contrato com relação a quaisquer disputas ou reivindicações decorrentes deste Adendo, incluindo disputas sobre sua existência, validade ou rescisão; e

12.2.2 este Adendo e todas as obrigações não contratuais ou outras decorrentes ou relacionadas a ele são regidas pelas leis do país ou território estipuladas para esse fim no Contrato.

Ordem de precedência

12.3 No caso de qualquer conflito ou inconsistência entre este Adendo e as Cláusulas Contratuais Padrão, onde as Cláusulas Contratuais Padrão são exigidas, as Cláusulas Contratuais Padrão prevalecerão.

12.4 Sujeito à seção 12.2, com relação ao assunto deste Adendo, no caso de inconsistências entre as disposições deste Adendo e quaisquer outros acordos entre as partes, incluindo o Contrato e incluindo (exceto quando explicitamente acordado por escrito, assinado em nome das partes) acordos firmados ou pretendidos celebrados após a data deste Adendo, as disposições deste Adendo prevalecerão.

Mudanças nas leis de proteção de dados

12.5 O cliente pode:

12.5.1 por meio de notificação por escrito de pelo menos trinta (30) dias corridos à Empresa, de tempos em tempos, proponha quaisquer variações nas Cláusulas Contratuais Padrão que sejam exigidas como resultado de qualquer alteração ou decisão de uma autoridade competente nos termos dessa Lei de Proteção de Dados; e

12.5.2 propor quaisquer outras variações deste Adendo que o Cliente considere razoavelmente necessárias para atender aos requisitos de qualquer Lei de Proteção de Dados.

12.6 Se o Cliente notificar de acordo com a seção 12.5, as partes discutirão imediatamente as variações propostas e negociarão de boa fé com o objetivo de concordar e implementar essas ou outras variações alternativas projetadas para atender aos requisitos identificados na notificação do Cliente assim que for razoavelmente praticável.

Separação

12.7 Caso alguma disposição deste Adendo seja inválida ou inexequível, o restante deste Adendo permanecerá válido e em vigor. A disposição inválida ou inexequível deve ser: (i) alterada conforme necessário para garantir sua validade e exequibilidade, preservando as intenções das partes da forma mais próxima possível ou, se isso não for possível; (ii) interpretada de forma como se a parte inválida ou inexequível nunca tivesse sido contida nela.

Anexo I — Detalhes do processamento de dados

Exportador de dados (Controlador): Cliente conforme identificado no Contrato.

Importador de dados (Processador): Empresa conforme identificada no Contrato.

Assunto: O assunto do processamento de dados sob este DPA são os Dados Pessoais do Cliente.

Duração do processamento: o prazo do Contrato mais o período até a Empresa excluir todos os Dados Pessoais do Cliente de acordo com este DPA.

Objetivo: O objetivo do processamento de dados é o fornecimento dos produtos e/ou serviços ao Cliente.

Natureza do processamento: A natureza do processamento de dados é para o fornecimento dos produtos e/ou serviços, conforme descrito no Contrato.

Categorias de titulares de dados: funcionários do cliente e funcionários de afiliados do cliente, clientes e parceiros de negócios.

Tipos de dados pessoais: o cliente pode carregar, enviar ou fornecer determinados dados pessoais do cliente aos produtos e/ou serviços, cuja extensão normalmente é determinada e controlada pelo cliente a seu exclusivo critério e pode incluir informações de contato; informações de interação com sites, produtos e serviços; endereços; data de nascimento; local de nascimento; endereço de e-mail; nomes; sexo; números de telefone; número da carteira de motorista; assinatura; número do funcionário; informações de geolocalização; taxa de pagamento; nome de usuário; senha; desempenho informações; qualificações e restrições; informações do dispositivo.

Dados confidenciais transferidos: Nenhum.

Frequência da transferência: contínua conforme necessário para o fornecimento dos produtos e/ou serviços.

Transferências para subprocessadores: conforme descrito na lista de subprocessadores da Empresa, disponível em https://commandalkon.com/sub-processor-list/.

Autoridade Supervisora Competente: Conforme determinado pelas Leis de Proteção de Dados aplicáveis ou, em ordem de vigência, 1) de acordo com os termos do Contrato ou 2) Autoridade de Proteção de Dados da Holanda.

Retenção: de acordo com o Contrato e este DPA.

Medidas **técnicas e organizacionais: As medidas** de segurança técnicas e organizacionais implementadas pelo importador de dados estão descritas na Seção 4.1 do DPA. Detalhes adicionais estão disponíveis mediante solicitação.