ADENDO SOBRE PROCESSAMENTO DE DADOS DA COMMAND ALKON INCORPORATED

Atualizado: 31/07/25

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

Este DPA substitui qualquer acordo anterior entre as partes em relação ao assunto aqui tratado, ou seja, privacidade e segurança de dados, conforme aplicável às Leis de Proteção de Dados (definidas abaixo).

Tendo em consideração as obrigações mútuas aqui estabelecidas, as partes concordam que os termos e condições abaixo estabelecidos serão adicionados como um aditamento ao Contrato.

1. Definições

"**Dados Pessoais do** Cliente" significa os 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 legislação/regulamentação adicional da Califórnia.

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

"**Estrutura de Privacidade de** Dados" ou "DPF" significa a estrutura jurídica da UE-EUA para transferências transfronteiriças de Dados Pessoais entre a União Europeia e os Estados Unidos e inclui a Extensão do Reino Unido à DPF UE-EUA e a DPF Suíça-EUA.

"Leis **de Proteção de** Dados" significa todas as leis e regulamentos aplicáveis relacionados ao Processamento de Dados Pessoais e privacidade que possam existir nas jurisdições relevantes, incluindo, quando aplicável, o Regulamento Geral sobre a Proteção de Dados (UE) 2016/679 relativo à proteção de pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE ("RGPD") (e qualquer alteração ou substituição do mesmo), a Lei Federal Suíça sobre Proteção de Dados ("FADP") (e qualquer alteração ou substituição da mesma), o RGPD da UE, conforme alterado e incorporado na legislação do Reino Unido ao abrigo da Lei do Reino Unido sobre a União Europeia (Saída) de 2018 e legislação secundária aplicável elaborada ao abrigo dessa lei ("RGPD do Reino Unido") (e qualquer alteração ou substituição da mesma), a Lei Canadiana de Proteção de Informações Pessoais e Documentos Eletrónicos ("PIPEDA") (e qualquer alteração ou substituição da mesma), a Lei Geral de Proteção de Dados do Brasil (a "LGPD") (e qualquer alteração ou substituição da mesma), a Lei de Privacidade de 1988 (Cth) da Austrália, conforme alterada ("Lei de Privacidade Australiana") (e qualquer alteração ou substituição da mesma), as leis estaduais de privacidade dos EUA (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 RGPD for especificamente mencionado, os mesmos requisitos serão aplicáveis 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 online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social do Titular dos Dados.

"Processar" ou "Processamento" significa qualquer operação ou conjunto de operações realizadas sobre os Dados Pessoais do Cliente, por meios automatizados ou não, tais como a recolha, registo, organização, estruturação, armazenamento, alteração, recuperação, consulta, utilização, divulgação, restrição, acesso, difusão, combinação, adaptação, cópia, transferência, apagamento e/ou destruição dos Dados Pessoais do Cliente.

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

"Cláusulas **Contratuais** Padrão" ou "SCCs" significa os requisitos contratuais padrão estabelecidos pela Lei de Proteção de Dados aplicável (Cláusulas Contratuais Padrão da UE, Cláusulas Contratuais Modelo Ibero-Americanas para Transferências Internacionais de Dados Pessoais, Cláusulas Contratuais Modelo da ASEAN para Fluxos Transfronteiriços de Dados, Cláusulas Contratuais Modelo de Hong Kong para Transferência Transfronteiriça de Dados Pessoais, Cláusulas Contratuais Padrão da SDAIA para Transferência de Dados Pessoais, etc.).

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

Os termos "controlador", "processador" e **"autoridade** supervisora", conforme utilizados neste DPA, terão os significados que lhes são atribuídos na Lei de Proteção de Dados aplicável.

Todos os outros termos não definidos, mas escritos com letra maiúscula, terão o significado estabelecido no Contrato ou na Lei de Proteção de Dados aplicável.

2. Tratamento dos Dados Pessoais do Cliente

2.1 Finalidade do processamento. A finalidade do processamento de dados nos termos deste DPA é o fornecimento dos produtos e/ou serviços de acordo com o Contrato. O Anexo 1 descreve o objeto e os detalhes do processamento dos Dados Pessoais do Cliente.

2.2 Responsabilidades do Processador e do Controlador. As partes reconhecem e concordam que: (a) a Empresa é um processador de Dados Pessoais do Cliente nos termos das Leis de Proteção de Dados; (b) o Cliente é um controlador de Dados Pessoais do Cliente nos termos das 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

que lhe são aplicáveis nos termos das Leis de Proteção de Dados com relação ao Processamento dos Dados Pessoais do Cliente.

2.3 Leis de Proteção de Dados dos EUA. Para os fins das Leis de Proteção de Dados dos EUA (incluindo a CCPA), "controlador" inclui "empresa"; "processador" inclui "prestador de serviços"; "Titular dos Dados" inclui "consumidor"; e "Dados Pessoais" inclui "informações pessoais". A Empresa é um prestador de serviços e o Cliente é uma empresa.

2.4 Instruções do 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 razoáveis por escrito fornecidas pelo Cliente, quando tais instruções forem consistentes com os termos do Contrato. O Cliente garantirá que suas instruções para o Processamento dos Dados Pessoais do Cliente estejam em conformidade com as Leis de Proteção de Dados. Entre as partes, o Cliente terá responsabilidade exclusiva 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 qualquer uma das instruções do Cliente entra em conflito com qualquer Lei de Proteção de Dados, a Empresa informará o Cliente dentro de um prazo razoável. A Empresa poderá Processar os Dados Pessoais do Cliente sem as instruções por escrito do Cliente se tal for exigido pela legislação aplicável à qual a Empresa está sujeita. Nessa situação, a Empresa informará o Cliente sobre tal exigência antes de Processar os Dados Pessoais do Cliente, a menos que tal seja proibido pela legislação aplicável.

2.6 Processamento CCPA. Na medida em que o Processamento de Dados Pessoais pela Empresa estiver sujeito à CCPA, a Empresa certifica que não irá: (a) reter, usar ou divulgar os Dados Pessoais do Cliente, exceto conforme previsto no Contrato, conforme necessário para fornecer os produtos e/ou serviços, para construir ou melhorar a qualidade dos produtos e/ou serviços, para detectar incidentes de segurança, para proteger contra atividades fraudulentas ou ilegais, para reter subprocessadores de acordo com este DPA ou conforme permitido pela CCPA; ou (b) vender ou compartilhar os Dados Pessoais do Cliente.

3. Subprocessadores

3.1 Nomeação de subprocessadores. O Cliente concede à Empresa autorização geral por escrito para contratar subprocessadores terceirizados para fornecer serviços limitados ou auxiliares relacionados ao fornecimento de produtos e/ou serviços. O site da Empresa lista os subprocessadores 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 uma solicitação na página de subprocessadores da Empresa (link acima) ou enviando tal solicitação paraprivacy@commandalkon.com . O Cliente pode se opor a qualquer subprocessador, comunicando tal objeção à Empresa dentro de trinta (30) dias após uma atualização, e as partes trabalharão de boa fé para resolver a objeção. O Cliente concorda com as atividades de subprocessamento realizadas pelos subprocessadores atuais listados no site da Empresa.

3.2 Segurança do subprocessador. Quando a Empresa subcontratar suas obrigações, ela deverá fazê-lo somente por meio de um contrato por escrito com o subprocessador que imponha obrigações contratuais pelo menos equivalentes às obrigações impostas à Empresa nos termos deste DPA. 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. Caso o subprocessador não cumpra suas obrigações de proteção de dados nos termos do referido contrato por escrito, a Empresa permanecerá totalmente responsável perante o Cliente pelo cumprimento das obrigações do subprocessador nos termos do referido contrato.

4. Responsabilidades de segurança do

4.1 Segurança da Empresa. A Empresa implementará medidas técnicas e organizacionais adequadas 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, o escopo, o contexto e as finalidades do Processamento, bem como o risco de variável probabilidade e gravidade para os direitos e liberdades das pessoas físicas. A Empresa de Segurança se rege pelas seguintes normas de segurança: SOC 2; 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 determinar de forma independente se os produtos e/ou serviços atendem aos requisitos e obrigações legais do Cliente, incluindo suas obrigações nos termos da Lei de Proteção de Dados aplicável. O Cliente é ainda responsável por configurar adequadamente os produtos e/ou serviços e utilizar os recursos e funcionalidades disponibilizados pela Empresa para manter a segurança adequada, tendo em conta a natureza dos Dados Pessoais do Cliente processados como resultado da utilização 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 de autenticação da conta, sistemas e dispositivos, e reter cópias dos Dados Pessoais do Cliente, conforme apropriado.

4.3 Pessoal da Empresa. A Empresa garantirá 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 adequado sobre suas responsabilidades e esteja sujeito a obrigações de confidencialidade, com tais obrigações sobrevivendo ao término do contrato do indivíduo com a Empresa.

4.4 Testes 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, caso o Cliente seja obrigado a realizar tais avaliações de impacto nos termos das 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, no uso ou recebimento dos 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 autorizada e capaz de fazê-lo. Se legalmente permitido, o Cliente será responsável por quaisquer custos decorrentes da prestação de tal assistência pela Empresa.

5.2 Obrigações de notificação. A Empresa deverá, na medida do permitido por lei, notificar imediatamente o Cliente se receber uma solicitação de um Titular dos Dados para acessar, corrigir, alterar, excluir ou contestar o Processamento dos Dados Pessoais do Cliente relacionados a tal indivíduo. A Empresa não responderá a qualquer 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 se refere ao Cliente. Além disso, a Empresa deverá, na medida do permitido por lei, notificar imediatamente o Cliente se receber uma solicitação de divulgação ou correspondência, notificação ou outra comunicação relacionada aos Dados Pessoais do Cliente por parte de autoridades policiais, autoridades competentes ou autoridades de proteção de dados relevantes. A Empresa fornecerá ao Cliente cooperação e assistência razoáveis e adequadas em relação ao tratamento de qualquer solicitação desse tipo, na medida do permitido por lei e na medida em que o Cliente não tenha acesso a tais Dados Pessoais do Cliente através do uso ou recebimento dos produtos e/ou serviços. Se permitido por lei, o Cliente será responsável por quaisquer custos decorrentes da prestação de tal 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 os Dados Pessoais do Cliente, a Empresa notificará o Cliente sobre a violação de segurança sem demora injustificada e, em qualquer caso, no prazo máximo de setenta e duas (72) horas após a confirmação. As obrigações desta Seção 6 não se aplicam a incidentes causados pelo Cliente ou pelo pessoal ou usuários finais do Cliente, nem a tentativas ou atividades malsucedidas que não

comprometam a segurança dos Dados Pessoais do Cliente, incluindo tentativas malsucedidas de login, pings, varreduras de porta, 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 enviada ao ponto de contato do Cliente por e-mail ou por telefone. É de responsabilidade exclusiva do Cliente garantir que as informações de contato nos sistemas de suporte da Empresa estejam sempre atualizadas. 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. Quando for necessária uma notificação, esta deverá, no mínimo e na medida do possível:

6.3.1 descrever a natureza da Violação de Segurança, as categorias e números de Titulares de Dados afetados e as categorias e números de registros de Dados Pessoais afetados;

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

6.3.3 descrever as consequências prováveis da Violação de Segurança; e

6.3.4 descrever as medidas tomadas ou propostas para resolver a Violação de Segurança.

7. Exclusão ou devolução dos dados pessoais do cliente

7.1 Excluir ou devolver. Sujeito à seção 7.3, a Empresa concorda em excluir de forma segura os Dados Pessoais do Cliente imediatamente e, em qualquer caso, no prazo de trinta (30) dias a partir da data de cessação de quaisquer serviços envolvendo o Processamento de Dados Pessoais do Cliente (a "Data de Cessação") ou, mediante solicitação por escrito do Cliente em tempo hábil, 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 Certificação por escrito. Se o Cliente e a Empresa tiverem celebrado Cláusulas Contratuais Padrão que exijam a certificação da exclusão por escrito (como as Cláusulas 8.5 e 16 das SCCs da UE), as partes concordam que a certificação por escrito só será fornecida mediante solicitação por escrito do Cliente.

7.3 Definição de Exclusão. Para esclarecimento, "Excluir" significa remover ou destruir 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 exigido 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 e

8.1 Direitos de auditoria. Não mais do que uma vez por ano, o Cliente pode contratar um terceiro mutuamente acordado para auditar os Dados Pessoais do Cliente exclusivamente para fins de cumprimento dos seus requisitos de auditoria, nos termos do Artigo 28, Secção 3(h) do RGPD ou qualquer disposição equivalente da Lei de Proteção de Dados aplicável. Para solicitar uma auditoria, o Cliente deve enviar um plano de auditoria detalhado com pelo menos quatro (4) semanas de antecedência da data proposta para a auditoria, descrevendo o âmbito, a duração e a data de início da auditoria. Os pedidos de auditoria devem ser enviados paraprivacy@commandalkon.com . O auditor deve assinar um acordo de confidencialidade por escrito aceitável para a Empresa antes de realizar a auditoria. A auditoria deve ser realizada durante o horário comercial normal, de acordo com as políticas da Empresa, e não pode interferir de forma injustificada nas atividades comerciais da Empresa. Quaisquer auditorias serão realizadas às custas e despesas exclusivas do Cliente. A Empresa cooperará com qualquer solicitação de auditoria do Cliente ou de qualquer autoridade regulatória ou supervisora competente para verificar o cumprimento das obrigações da Empresa nos termos deste DPA, disponibilizando, sujeito a obrigações de confidencialidade, 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 em matéria de conformidade. Tendo em conta a natureza do Tratamento e as informações disponíveis à Empresa, a Empresa prestará cooperação e assistência adequadas e razoáveis ao Cliente no que diz respeito às obrigações de conformidade do Cliente descritas nos artigos 32.º a 36.º do RGPD.

9. Transferências de dados

9.1 Autorização geral. O Cliente concorda que a Empresa pode, sujeito à Seção 9.2, armazenar e Processar os Dados Pessoais do Cliente nos Estados Unidos da América e em qualquer outro país em que a Empresa ou qualquer um de seus subprocessadores mantenha instalações ou de outra forma Processe Dados Pessoais. Quaisquer transferências serão regidas primeiro pela certificação da Estrutura de Privacidade de Dados da Empresa ou, alternativamente, pelas Cláusulas Contratuais Padrão entre afiliadas 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 em conformidade com a lei aplicável, e não fará com que o Cliente viole qualquer Lei de Proteção de Dados.

9.2 Cláusulas Contratuais Padrão da UE. Na medida em que, e apenas na medida em que, a Empresa processar Dados Pessoais do Cliente do Espaço Econômico Europeu e forem necessárias Cláusulas Contratuais Padrão, o Módulo Dois das Cláusulas Contratuais Padrão será aplicável e está incorporado neste documento. Para os fins das Cláusulas Contratuais Padrão, o Cliente é o "exportador de dados" e a Empresa é o "importador de dados".

9.3 Adendo do Reino Unido às Cláusulas Contratuais Padrão da UE. Na medida em que, e apenas na medida em que, a Empresa processar Dados Pessoais de Clientes do

Reino Unido e forem necessárias Cláusulas Contratuais Padrão, as partes concordam que o Adendo do Reino Unido se aplicará aos Dados Pessoais que forem transferidos através dos produtos e/ou serviços do Reino Unido, seja diretamente ou através 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 do Reino Unido como fornecendo um nível adequado de proteção para Dados Pessoais.

9.4 FADP suíço. Na medida em que, e apenas na medida em que, a Empresa processar dados pessoais de clientes da Suíça, os seguintes requisitos adicionais serão aplicáveis na medida em que as transferências de dados estiverem exclusivamente sujeitas à FADP ou estiverem sujeitas tanto à FADP quanto ao RGPD da UE: (a) o termo "Estado-Membro" não deve ser interpretado de forma a excluir os Titulares dos Dados na Suíça da possibilidade de exercerem os seus direitos no seu local de residência habitual (Suíça), em conformidade com a Cláusula 18(c) das Cláusulas Contratuais Padrão; (b) na medida em que as transferências de dados subjacentes às Cláusulas Contratuais Padrão estejam exclusivamente sujeitas à FADP, as referências ao RGPD da UE devem ser entendidas como referências à FADP; e (c) na medida em que as transferências de dados subjacentes às Cláusulas Contratuais Padrão estejam sujeitas tanto à FADP quanto ao RGPD da UE, as referências ao RGPD da UE devem ser entendidas como referências à FADP, na medida em que as transferências de dados estejam sujeitas à FADP.

9.5 Outras Cláusulas Contratuais Padrão ou Cláusulas Contratuais Modelo. Na medida em que, e apenas na medida em que, houver uma transferência de Dados Pessoais do Cliente além daqueles discutidos acima que exija SCCs ou Cláusulas Contratuais Modelo específicas para cada país de acordo com as Leis de Proteção de Dados aplicáveis, as partes concordam que as SCCs ou Cláusulas Contratuais Modelo específicas para cada país, conforme necessário, são automaticamente incorporadas por referência e fazem parte integrante deste DPA.

9.6 Medidas complementares. Em complemento às Cláusulas Contratuais Padrão, se a Empresa tomar conhecimento de que qualquer autoridade governamental (incluindo autoridades policiais) deseja obter acesso ou uma cópia de alguns ou todos os Dados Pessoais do Cliente processados pela Empresa, seja de forma voluntária ou obrigatória, para fins relacionados à inteligência de segurança nacional, então, a menos que seja legalmente proibido ou sob uma obrigação legal que exija o contrário, a Empresa irá: 1) notificar imediatamente o Cliente a quem os Dados Pessoais se aplicam; 2) informar à autoridade governamental relevante que não foi autorizada a divulgar os Dados Pessoais do Cliente e, a menos que seja legalmente proibido, precisará notificar imediatamente o Cliente a quem os Dados Pessoais do Cliente se aplicam; 3) informar à autoridade governamental que ela deve encaminhar todas as solicitações ou exigências 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 obrigação. Se a Empresa for obrigada a apresentar os Dados Pessoais do Cliente, a

Empresa só divulgará os Dados Pessoais do Cliente na medida do legalmente necessário, de acordo com o processo legal aplicável.

9.7 Lei de Vigilância de Inteligência Estrangeira. A Empresa não recebeu anteriormente qualquer diretiva ao abrigo da Secção 702 da Lei de Vigilância de Inteligência Estrangeira dos EUA, codificada em 50 U.S.C. §1881a ("FISA Secção 702"). Nenhum tribunal considerou a Empresa como sendo o tipo de entidade elegível para receber processos emitidos nos termos da Seção 702 da FISA. A Empresa não é o tipo de provedor elegível para ser sujeito a coleta upstream (coleta "em massa") nos termos da Seção 702 da FISA, conforme descrito na decisão *Schrems II*.

9.8 Precedência da transferência. No caso de os serviços serem abrangidos 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 exigido 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, não obstante o término do prazo de qualquer assinatura adquirida, permanecerá em vigor até e expirará automaticamente após a exclusão de todos os Dados Pessoais do Cliente, conforme descrito neste DPA.

11. Não conformidade; Recursos; Partes

11.1 Limitação de responsabilidade. A responsabilidade da Empresa pelo incumprimento das suas obrigações no presente DPA está sujeita à disposição de limitação de responsabilidade prevista no Contrato.

11.2 Partes deste DPA. Nada neste DPA conferirá quaisquer benefícios ou direitos a qualquer pessoa ou entidade que não seja parte deste DPA.

12. Termos gerais

Lei aplicável e jurisdição

12.1 Este DPA será revisto conforme apropriado, de acordo com as circunstâncias.

12.2 Sem prejuízo das cláusulas 7 (Mediação e Jurisdição) e 9 (Lei Aplicável) das Cláusulas Contratuais Padrão:

12.2.1 as partes deste DPA, por meio deste, se submetem à escolha da jurisdição estipulada no Contrato com relação a quaisquer disputas ou reclamações que possam surgir sob este DPA , incluindo disputas relativas à sua existência, validade ou rescisão; e

12.2.2 este DPA e todas as obrigações extracontratuais ou outras obrigações decorrentes ou relacionadas com o mesmo são regidas pelas leis do país ou território estipulado para esse efeito no Contrato.

Ordem de precedência

12.3 Em caso de conflito ou inconsistência entre este DPA e as Cláusulas Contratuais Padrão, quando estas forem exigidas, prevalecerão as Cláusulas Contratuais Padrão.

12.4 Sujeito às seções 12.2 e 12.3, no que diz respeito ao objeto deste DPA, em caso de inconsistências entre as disposições deste DPA e quaisquer outros acordos entre as partes, incluindo o Contrato e incluindo (exceto quando explicitamente acordado de outra forma por escrito, assinado em nome das partes) acordos celebrados ou que se pretenda celebrar após a data deste DPA, prevalecerão as disposições deste DPA.

Alterações nas leis de proteção de dados

12.5 O Cliente pode:

12.5.1 mediante notificação por escrito com antecedência mínima de trinta (30) dias úteis à Empresa, propor quaisquer alterações às Cláusulas Contratuais Padrão que sejam necessárias em resultado de qualquer alteração ou decisão de uma autoridade competente ao abrigo da Lei de Proteção de Dados; e

12.5.2 propor quaisquer outras alterações a este DPA que o Cliente considere razoavelmente necessárias para atender aos requisitos de qualquer Lei de Proteção de Dados.

12.6 Se o Cliente enviar uma notificação nos termos da seção 12.5, as partes deverão discutir prontamente as alterações propostas e negociar de boa-fé com o objetivo de chegar a um acordo e implementar essas alterações ou alterações alternativas destinadas a atender aos requisitos identificados na notificação do Cliente, assim que for razoavelmente possível.

Rescisão

12.7 Caso qualquer disposição deste DPA seja inválida ou inexequível, o restante deste DPA permanecerá válido e em vigor. A disposição inválida ou inexequível será: (i) alterada conforme necessário para garantir sua validade e exequibilidade, preservando as intenções das partes da forma mais fiel possível ou, se isso não for possível; (ii) interpretada de forma que a parte inválida ou inexequível nunca tenha sido incluída no documento.

Anexo I – Detalhes do processamento de dados

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

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

Objeto: O objeto do Tratamento de Dados nos termos deste DPA são os Dados Pessoais do Cliente.

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

Finalidade: A finalidade do tratamento 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 descritos no Contrato e neste DPA.

Categorias de titulares dos dados: Funcionários do Cliente e funcionários de afiliadas do Cliente, clientes e parceiros comerciais.

Tipos de dados pessoais: O Cliente pode carregar, enviar ou fornecer determinados Dados Pessoais do Cliente aos produtos e/ou serviços, cuja extensão é normalmente determinada e controlada pelo Cliente a seu exclusivo critério e pode incluir informações de contato; informações sobre interação com o site, produto e serviço; endereços; data de nascimento; local de nascimento; endereços de e-mail; nomes; sexo; cargo; números de telefone; número da carteira de motorista; assinatura; número de funcionário; informações de geolocalização; taxa de remuneração; nome de usuário; senha; informações de desempenho; qualificações e restrições; informações sobre dispositivos.

Dados sensíveis transferidos: Nenhum.

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

Transferências para subprocessadores: Conforme descrito neste DPA e na lista de subprocessadores da Empresa disponível em . Registros das atividades de processamento disponíveis mediante solicitação.

Autoridade Supervisora Competente: Conforme determinado pelas Leis de Proteção de Dados aplicáveis ou, por ordem de efeito, 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.