DATA PROCESSING AGREEMENT

Este Data Processing Agreement ("**DPA**") é parte indissociável do Master Services Agreement encontrado em https://vtex.com/us-en/agreements/, a menos que a Contratante tenha celebrado outro acordo por escrito com a VTEX que prevaleça sobre o Master Services Agreement. O Master Service Agreement e a Proposta Comercial são denominados, em conjunto, "**Contrato**".

Apenas para os fins deste DPA, e exceto onde indicado de outra forma, o termo "Contratante" deve incluir a Contratante e as Afiliadas da Contratante que, pelas Leis de Proteção de Dados, devam celebrar um DPA com a VTEX. Todos os termos em maiúsculas não definidos neste instrumento terão o significado estabelecido no Contrato.

Ao assinar este adendo, a Contratante celebra este DPA em seu nome e, na medida em que as Leis de Proteção de Dados assim o exijam, em nome de qualquer Afiliada do Contratante (conforme definido abaixo) que seja um terceiro beneficiário nos termos do Contrato.

Durante a prestação dos Serviços previstos no Contrato, a VTEX pode Tratar determinados Dados Pessoais (definidos abaixo) em nome da Contratante; e quando a VTEX Tratar tais Dados Pessoais em nome da Contratante, as Partes concordam em cumprir os termos e condições deste DPA em relação ao Tratamento de Dados Pessoais.

COMO ASSINAR ESTE DPA?

1. Este DPA consiste em duas partes: o conteúdo principal do DPA e seus 2 anexos:
   - **Anexo 1 - Descrição do Tratamento:** O Anexo 1 contém a descrição das atividades de Tratamento relacionados aos Serviços prestados pela VTEX nos termos do Contrato.
   - **Anexo 2: Medidas técnicas e organizacionais**

2. As Leis de Proteção de Dados (conforme definido abaixo) podem exigir que as obrigações deste DPA e seus Anexos sejam complementadas por disposições adicionais ou alternativas para garantir a conformidade com as respectivas Leis de Proteção de Dados ("Termos Especiais").

3. A Contratante declara estar ciente das cláusulas previstas neste DPA ao assinar a Proposta Comercial.

COMO ESTE DPA SE APLICA À CONTRATANTE E SUAS AFILIADAS?

Se a entidade da Contratante que assina este DPA for a Contratante prevista no Contrato, este DPA é um adendo e faz parte do Contrato. Se a Afiliada da Contratante for uma parte deste DPA nos termos da cláusula 8 abaixo, este DPA vincula a VTEX e esta Afiliada da Contratante. Nesse caso, as referências a "VTEX" neste DPA significarão a entidade VTEX que é parte do Contrato.

Se a entidade da Contratante que assina este DPA assinou uma Proposta Comercial com a VTEX ou sua Afiliada, nos termos do Contrato, mas não é parte do Contrato, este DPA é um adendo a essa Proposta Comercial e respectivas renovações. Referências a "VTEX" neste DPA significam a entidade VTEX que é parte de tal Proposta Comercial.

1. TERMOS DEFINIDOS

Para os fins deste DPA, quaisquer termos em letras maiúsculas que não estejam definidos abaixo ou de outra forma neste DPA ou nas Leis de Proteção de Dados aplicáveis terão os significados atribuídos a eles no Contrato.

“**Afiliada**” significa qualquer entidade que direta ou indiretamente controle, seja controlada ou esteja sob controle comum com a entidade em questão. “Controle”, para os fins deste termo definido, significa propriedade ou controle direto ou indireto de mais de 50% das participações societárias com direito a voto da entidade em questão.

"Afiliada da Contratante" significa qualquer Afiliada da Contratante (a) (i) que esteja sujeita às Leis de Proteção de Dados, e (ii) autorizada a utilizar os Serviços de acordo com o Contrato entre a Contratante e a VTEX, mas não assinaram sua própria Proposta Comercial e não são uma “Contratante” conforme definido no Contrato; (b) se e na medida em que a VTEX trata Dados Pessoais em relação aos quais tal(is) Afiliada(s) se qualifica(m) como Controlador.

“**Autoridade Supervisora**” significa o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, nos termos do art. 5, XIX, e qualquer autoridade reguladora similar responsável pela aplicação das Leis de Proteção de Dados.

“**Contratante**” significa a parte contratante do Contrato e que assina este DPA em seu nome, e em nome de toda e qualquer Afiliada da Contratante, conforme o caso.

“**Controlador**” significa a entidade que determina as finalidades e os meios do Tratamento de Dados Pessoais. Para os fins deste DPA, o Controlador é a Contratante (conforme definido no Contrato) e/ou qualquer Afiliada do Contratante.

“**Dados da Contratante**” significa todos os dados e informações enviados por Usuários Autorizados no contexto dos Serviços, incluindo textos de mensagem, arquivos, comentários e links, excluindo-se produtos da Contratante. Dados da Contratante não incluem: quaisquer Dados Pessoais relativos aos Usuários Autorizados recebidos para fins de autorização de acesso aos Serviços; ou Dados Pessoais dos representantes da Contratante ou de Afiliadas da Contratante envolvidos com a operação e administração do Contrato ou deste DPA, os quais a VTEX trata na posição de controlador.

“**Dados Pessoais**” significa quaisquer Dados da Contratante relacionados a uma pessoa física identificada ou identificável, desde que tais informações sejam protegidas como dados pessoais pelas Leis de Proteção de Dados aplicáveis.

“**Grupo VTEX**” significa a VTEX e suas Afiliadas envolvidas no Tratamento de Dados Pessoais.

“**Incidente de Dados Pessoais**” significa um incidente de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou tratados.

“**LGPD**” significa a Lei Nº 13.709 de 14/08/2018 (Lei Geral de Proteção de Dados).

“**Usuários Autorizados**” significa qualquer pessoa autorizada pela VTEX, por escrito, a ter controle sobre o ambiente da Plataforma VTEX; e qualquer pessoa que tenha acesso autorizado pela Contratante ao ambiente da Plataforma VTEX, conforme as condições previstas no Contrato.

“**Leis de Proteção de Dados**” significa (i) a LGPD, (ii) qualquer legislação em vigor em qualquer outra jurisdição aplicável ao Contrato; e (iii) quaisquer orientações ou códigos de prática emitidos ou adotados por qualquer Autoridade Supervisora ou órgão de proteção de dados competente, conforme aplicável às atividades Tratamento de Dados Pessoais nos termos do Contrato e conforme atualizado, alterado, substituído ou revogado.

“**Operador”** significa a entidade que Trata Dados Pessoais em nome do Controlador. Para os fins deste DPA, o Operador é a VTEX.

“**Sub-operador**” significa qualquer entidade contratada pela VTEX, incluindo um membro do Grupo VTEX, como sub-operador, para Tratar Dados Pessoais na realização dos Serviços.

“**Titular**” significa a pessoa física identificada ou identificável a quem os Dados Pessoais se referem.

"**Tratamento**" significa qualquer operação ou conjunto de operações que seja realizada em Dados Pessoais, seja por meios automáticos ou não, tais como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

"**VTEX**" significa a entidade VTEX que é parte deste DPA, conforme especificado na seção "COMO ESTE DPA SE APLICA À CONTRATANTE E SUAS AFILIADAS" acima.

2. TRATAMENTO DE DADOS PESSOAIS

2.1. **Funções das Partes**. As partes reconhecem e concordam que, com relação ao Tratamento de Dados Pessoais no contexto do Contrato, a Contratante é a Controladora, a VTEX é a Operadora, e que a VTEX contratará Sub-operadores de acordo com os requisitos estabelecidos na Cláusula 4 "Sub-operadores" abaixo. As partes concordam que, na medida em que a VTEX e/ou qualquer Afiliada da VTEX esteja atuando como Controlador em relação aos Dados Pessoais dos contatos comerciais da Contratante, e a Contratante esteja atuando como Controladora em relação aos Dados Pessoais dos contatos comerciais da VTEX, cada um atua como um Controlador separado e independente da Contratante e/ou Afiliadas da Contratante.

2.2. **Tratamento de Dados Pessoais da Contratante.** A Contratante deverá, em seu uso dos Serviços e fornecimento de instruções à VTEX, Tratar Dados Pessoais de acordo com os requisitos das Leis de Proteção de Dados. A Contratante será a única responsável pela exatidão, qualidade e legalidade dos Dados Pessoais e pelos meios pelos quais a Contratante adquiriu os Dados Pessoais fornecidos à VTEX. A Contratante garante que possui base legal e consentimento, quando necessário, dos Titulares para compartilhar os Dados Pessoais com a VTEX; e para a VTEX tratar os Dados Pessoais conforme contemplado no Contrato e neste DPA.

2.3. **Tratamento de Dados Pessoais da VTEX**. Como Operador da Contratante, a VTEX e qualquer pessoa agindo sob sua autoridade ou de uma Afiliada da VTEX que tenha acesso a Dados Pessoais, somente tratará Dados Pessoais de acordo com as Leis de Proteção de Dados (conforme aplicável aos Operadores) e cumprirá todas as obrigações aplicáveis a Operadores sob tais leis e devem:

(i) Tratar os Dados Pessoais da Contratante de acordo com o Contrato, inclusive para o fornecimento e manutenção dos Serviços e para o uso dos Serviços pelos Usuários Autorizados;

(ii) Tratar os Dados Pessoais decorrentes do uso dos Serviços por Usuários Autorizados; e

(iii) Tratar os Dados Pessoais da Contratante de acordo com instruções razoáveis e documentadas fornecidas pela Contrante (por exemplo, por e-mail ou tickets de suporte) que sejam consistentes com os termos do Contrato (individual e coletivamente, a "**Finalidade**");

(iv) Não Tratar esses Dados Pessoais, exceto por instruções da Contratante, ou a menos que exigido pela LGPD ou quaisquer Leis de Proteção de Dados às quais o Operador esteja sujeito, caso em que a VTEX ou a Afiliada da VTEX informará à Contratante, ou a Afiliada da Contratante, dessa obrigação legal antes do Tratamento; a menos que essa lei proíba por razões de interesse público. Ao tratar Dados Sensíveis, conforme definido no Anexo 1, ou Categorias de Dados nativas a processos que foram personalizados pelo Controlador, a responsabilidade da VTEX é limitada ao armazenamento desses dados. Este DPA e o Contrato são as instruções completas e finais da Contratante no momento da celebração do DPA para o Tratamento de Dados Pessoais. Quaisquer instruções adicionais ou alternativas devem ser solicitadas separadamente por escrito à VTEX; e

(v) informar à Contratante ou Afiliada da Contratante se, na opinião da VTEX ou da Afiliada da VTEX, as instruções dadas pelo Controlador infringirem as Leis de Proteção de Dados.

2.4**. Detalhes do Tratamento.** A finalidade do Tratamento de Dados Pessoais pela VTEX está descrita na Finalidade na Cláusula 2.3. A duração do Tratamento, a natureza e a finalidade do

Tratamento, os tipos de Dados Pessoais e as categorias de Titulares de Dados Tratados sob este DPA são especificados no Anexo 1 (Descrição das Atividades de Tratamento) deste DPA.

3. DIREITOS DOS TITULARES DE DADOS

3.1. **Solicitações dos Titulares dos Dados**. A VTEX deverá, na extensão permitida na LGPD, notificar sem demora a Contratante se a VTEX receber qualquer solicitação de um Titular para exercer seus direitos previstos nas Leis de Proteção de Dados em relação a Dados Pessoais: acesso, retificação, restrição de Tratamento, eliminação, portabilidade de dados, objeção ao Tratamento ou não estar sujeito a decisões automatizadas, bem como quaisquer direitos previstos nas Leis de Proteção de Dados aos Titulares (cada uma, "**Solicitação de Titular**"). Levando em consideração a natureza do Tratamento, a VTEX auxiliará a Contratante por meio de medidas técnicas e organizacionais apropriadas, na medida do possível, para o cumprimento da obrigação da Contratante de responder a uma Solicitação de Titular. Além disso, na medida em que a Contratante, em seu uso dos Serviços, não tenha a capacidade de atender a uma Solicitação do Titular, a VTEX deverá, mediante instrução da Contratante, fornecer esforços comercialmente razoáveis para ajudar a Contratante a responder a tal Solicitação do Titular, desde que a resposta a tal Solicitação de Titular seja exigida pelas Leis de Proteção de Dados. A Contratante será responsável por quaisquer custos decorrentes da prestação de tal assistência pela VTEX caso solicite funcionalidade(s) adicional(is).

4. SUB-OPERADORES

4.1. **Contratação de Sub-operadores**. A Contratante reconhece e concorda que (a) as Afiliadas da VTEX podem ser Sub-operadores nos termos deste DPA e (b) a VTEX e as Afiliadas da VTEX, respectivamente, podem contratar Sub-operadores terceirizados, em relação à prestação dos Serviços. Como condição para permitir que um Sub-operadores Trate Dados Pessoais, a VTEX (ou uma Afiliada da VTEX atuando como Sub-operador) celebrará um contrato por escrito com cada Sub-operador, contendo obrigações de proteção de dados que forneçam pelo menos o mesmo nível de proteção para Dados Pessoais quanto neste DPA, na medida aplicável à natureza dos Serviços prestados e os Dados Pessoais tratados por tais Sub-operadores.

4.2. **Lista de Sub-operadores Atuais e Notificação de Novos Sub-operadores**. Uma lista atual de Sub-operadores contratados pela VTEX para a prestação dos Serviços, incluindo as identidades desses Sub-operadores e seu país de localização, está disponível no Anexo 1 deste DPA. Essa lista pode ser atualizada e permanecerá acessível em https://vtex.com/us-en/privacy-and-agreements/subprocessors/ ("**Lista de Sub-operadores**"). A VTEX deverá manter uma Lista atualizada de Sub-operadores antes de serem autorizados a Tratar Dados Pessoais em relação à prestação dos Serviços.

5. SEGURANÇA

5.1. **Controles para a Proteção de Dados Pessoais**. A VTEX manterá as medidas técnicas e organizacionais adequadas para proteção da segurança, confidencialidade e integridade dos Dados Pessoais no contexto da prestação dos Serviços. As medidas atuais da VTEX estão estabelecidas no **Anexo 2** deste DPA e podem ser alteradas periodicamente para manter a conformidade com este DPA e/ou Leis de Proteção de Dados. Uma versão atualizada das medidas de segurança pode ser encontrada no ambiente admin da Contratante. A VTEX monitora regularmente o cumprimento dessas medidas. A VTEX não diminuirá substancialmente a segurança geral dos Serviços durante o período de assinatura.

5.2. **Certificações e Auditorias de Terceiros**. A VTEX obteve as certificações e auditorias de terceiros estabelecidas no Portal Trust Hub (https://vtex.com/us-en/compliance/). Mediante solicitação da Contratante, e sujeito às obrigações de confidencialidade previstas no Contrato, a VTEX disponibilizará à Contratante (ou auditor terceirizado independente da Contratante) informações sobre o cumprimento do Grupo VTEX das obrigações previstas neste DPA, na forma de as certificações e auditorias de terceiros estabelecidas no Portal Trust Hub (https://vtex.com/us-en/compliance/). A Contratante pode solicitar à VTEX uma auditoria presencial na VTEX referente à proteção de Dados Pessoais no contexto dos Serviços, mas apenas na medida exigida pelas Leis de Proteção de Dados. A Contratante reembolsará a VTEX por qualquer tempo gasto em qualquer auditoria no local, conforme preços aplicáveis ao Grupo VTEX na ocasião, que serão disponibilizadas à Contratante mediante solicitação. Antes do início de qualquer auditoria no local, a Contratante e a VTEX devem concordar mutuamente sobre o escopo, tempo e duração da auditoria e quaisquer medidas para proteger a segurança de dados pessoais de terceiros ou informações confidenciais da VTEX, além do pagamento dos custos a serem arcados pela a Contratante. Todos os custos devem ser razoáveis, levando em consideração os recursos despendidos pela VTEX. A Contratante deverá notificar prontamente a VTEX sobre qualquer não conformidade descoberta durante uma auditoria, e a VTEX deverá envidar esforços comercialmente razoáveis para resolver qualquer não conformidade confirmada.

6. GESTÃO E NOTIFICAÇÃO DE INCIDENTES DE DADOS PESSOAIS

A VTEX mantém políticas e procedimentos de gerenciamento de incidentes de segurança especificados no ambiente admin da Contratante.

A VTEX notificará a Contratante sem demora indevida sobre quaisquer Incidentes de Dados Pessoais da qual a VTEX tome conhecimento conforme exigido pelas Leis de Proteção de Dados. A VTEX fornecerá cooperação e assistência comercialmente razoáveis na identificação da causa de tal Incidente de Dados Pessoais e tomará medidas comercialmente razoáveis para auxiliar na investigação, contenção e remediação, incluindo medidas para mitigar seus efeitos adversos, na medida em que a remediação esteja sob o controle da VTEX. A VTEX deverá documentar qualquer Incidente de Dados Pessoais, incluindo os fatos relacionados à Violação de Dados Pessoais, seus efeitos e a ação corretiva implementada pela VTEX, desde que a correção esteja sob o controle da VTEX.

7. DEVOLUÇÃO E EXCLUSÃO DE DADOS PESSOAIS

A VTEX deverá, mediante solicitação da Contratante em até 30 dias antes da extinção do Contrato e sujeita às limitações descritas no Contrato e no ambiente admin da Contratante, fornecer os meios para a Contratante extrair uma cópia completa de todos os Dados Pessoais da Contratante sob posse da VTEX ou, na ausência de quaisquer instruções da Contratante, destruir com segurança esses Dados Pessoais, demonstrando por comprovante escrito à Contratante que tomou tais medidas; exceto se a lei aplicável a impeça de devolver ou destruir os Dados Pessoais total ou parcialmente, ou exigir armazenamento dos Dados Pessoais, caso em que a VTEX garante que continuará a garantir o cumprimento deste DPA, e apenas tratará os dados na medida e pelo período exigido pela lei aplicável. A Contratante reconhece que a VTEX pode cumprir a obrigação acima fornecendo as interfaces necessárias à Contratante para extrair os Dados Pessoais por seus próprios meios. A Contratante deverá arcar com eventuais custos para extração de dados não realizada por autoatendimento.

8. AFILIADAS DA CONTRATANTE

8.1. **Relação contratual**. As partes reconhecem e concordam que, ao assinar o DPA, a Contratante celebra o DPA em seu próprio nome e, conforme aplicável, em nome das Afiliadas da Contratante, formalizando assim um DPA separado entre a VTEX e cada Afiliada da Contratante sujeita às disposições do Contrato e da Cláusula 8 deste DPA. A Contratante garante que tem o poder e a autoridade para celebrar o DPA em seu próprio nome e, conforme aplicável, em nome das Afiliadas da Contratante. Cada Afiliada da Contratante concorda em cumprir as obrigações deste DPA e do Contrato, quando aplicável. Para evitar dúvidas, uma Afiliada da Contratante não é e não se torna parte do Contrato, é apenas parte do DPA. Todo acesso e uso dos Serviços por Afiliadas da Contratante deve cumprir os termos e condições do Contrato e deste DPA, e qualquer violação dos termos e condições do Contrato e deste DPA por uma Afiliada da Contratante, será considerada uma violação pela Contratante.

8.2. **Comunicação**. A Contratante que é parte contratante do Contrato permanecerá responsável por coordenar todas as comunicações com a VTEX nos termos do Contrato e deste DPA, e terá o direito de fazer e receber qualquer comunicação em relação a este DPA em nome de suas Afiliadas.

8.3. **Direitos das Afiliadas da Contratante**. Se uma Afiliada da Contratante se tornar parte do DPA com a VTEX, ela poderá, na extensão exigida pelas Leis de Proteção de Dados, também ter o direito de exercer direitos nos termos deste DPA, sujeito ao seguinte:

8.3.1. Exceto se as Leis de Proteção de Dados exigirem que a Afiliada da Contratante exerça um direito ou nos termos deste DPA contra a VTEX diretamente, as partes concordam que (i) somente a Contratante que é a parte do Contrato exercerá tal direito em nome da Afiliada da Contratante, e (ii) a Contratante que é a parte do Contrato exercerá tais direitos nos termos deste DPA, não para cada Afiliada da Contratante individualmente, mas de maneira combinada para todas as Afiliadas da Contratante (conforme previsto, por exemplo, na Cláusula 8.3.2, abaixo).

8.3.2. As partes concordam que a Contratante que é a parte do Contrato deverá, se realizar uma auditoria na VTEX em relação à proteção de Dados Pessoais, tomar todas as medidas razoáveis para limitar qualquer impacto na VTEX, combinando, para na medida do possível, várias solicitações de auditoria em nome de diferentes Afiliadas da Contratante em uma única auditoria.

9. LIMITAÇÃO DE RESPONSABILIDADE

A responsabilidade de cada parte e de todas as suas Afiliadas, em conjunto, decorrente ou relacionada a este DPA, e todas os DPAs entre as Afiliadas da Contratante e a VTEX, incluindo, de maneira não exaustiva, danos diretos, indiretos, morais, punitivos, danos emergentes, lucros cessantes, perda de oportunidade e perda de dados, está sujeita à cláusula 'Responsabilidade Limitada da VTEX' do Contrato, e qualquer referência à responsabilidade de uma parte significa a responsabilidade agregada dessa parte e de todas as suas Afiliadas com base no Contrato e todos os DPAs, em conjunto.

Para evitar dúvidas, a responsabilidade total da VTEX e de suas Afiliadas por todas as demandas da Contratante e suas Afiliadas decorrentes ou relacionadas ao Contrato e o DPA deve ser aplicada em conjunto para todas as demandas com base no Contrato e no DPA e, em particular, não deve ser entendido como aplicável individual e individualmente à Contratante e/ou a qualquer Afiliada da Contratante que seja parte do DPA.

10. OUTRAS DISPOSIÇÕES - LEI BRASILEIRA

10.1. **Leis de Proteção de Dados**. A VTEX trata os Dados Pessoais de acordo com as Leis de Proteção de Dados na medida diretamente aplicável à prestação dos Serviços pela VTEX.

10.1.1. **Avaliação do Impacto da Proteção de Dados**. Mediante solicitação da Contratante, a VTEX fornecerá à Contratada cooperação e assistência razoáveis necessárias para cumprir as obrigações da Contratante previstas nas Leis de Proteção de Dados a fim de realizar uma avaliação de impacto de proteção de dados relacionada ao uso dos Serviços pela Contratante, no qual uma atividade de tratamento possa resultar em uma alto risco para os direitos e liberdades dos titulares, na medida em que a Contratante não tenha acesso às informações necessários, e que essas informações estejam disponíveis para a VTEX. A VTEX fornecerá assistência razoável à Contratante para consultar a Autoridade Supervisora, antes do Tratamento, na extensão exigida pelas Leis de Proteção de Dados.

10.1.2. A VTEX notificará a Contratante se acreditar que uma instrução infringe quaisquer Leis de Proteção de Dados.

10.1.3. Transferências restritas. As Partes reconhecem que, ao fornecer os Serviços, a VTEX transferirá Dados Pessoais para destinatários (incluindo parceiros e Sub-operadores da VTEX) que possam estar localizados fora do Brasil. Esses países podem não oferecer um nível adequado de proteção de dados, conforme definido pelas Leis de Proteção de Dados. Consequentemente, tais transferências de Dados Pessoais serão protegidas por salvaguardas apropriadas exigidas pela LGPD, incluindo cláusulas padrão determinadas pela Autoridade Supervisora (Art.33, II, b, LGPD) ou, na falta de instruções dessa Autoridade, as cláusulas contratuais padrão aprovadas pela Comissão Europeia aprovadas na Decisão EU 2021/914 de 4 de junho de 2021 ("**Transferência Restrita**").

10.1.3.1 Se, a qualquer momento, uma Autoridade Supervisora ou um tribunal com jurisdição competente sobre uma parte determinar que as transferências de Controladores no Brasil para Operadores fora do Brasil devam estar sujeitas a salvaguardas adicionais específicas (incluindo, mas não se limitando a medidas técnicas e organizacionais específicas), as Partes trabalharão juntas de boa fé para implementar tais salvaguardas e garantir que qualquer transferência de Dados Pessoais da Contratada seja realizada com base em tais salvaguardas adicionais.

10.1.4. **Transferências para sub-operadores**. As Partes reconhecem que, ao prestar os Serviços, a VTEX realizará Transferências Restritas para Sub-operadores, conforme cláusula 10.1.3 deste DPA.

10.1.5. **Confidencialidade**. A VTEX garantirá que as pessoas autorizadas a Tratar Dados Pessoais estejam sujeitas a uma obrigação contratual ou legal que assegure a confidencialidade.

11. EFICÁCIA

Este DPA será eficaz perante a Contratante e a VTEX quando as etapas previstas na Cláusula "COMO ASSINAR ESTE DPA" acima forem totalmente concluídas. Se a Contratante já tiver assinado anteriormente um adendo de processamento de dados com a VTEX, este DPA substitui e substitui o adendo de processamento de dados anterior.

12. LEI APLICÁVEL

Conforme estabelecido na Cláusula "Lei Aplicável" no Master Service Agreement.

13. ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS

A descrição do Tratamento dos Dados Pessoais da Contratante; a duração do Tratamento; a natureza e finalidade do Tratamento dos Dados Pessoais da Contratante; e os detalhes das obrigações e direitos da Contratante e da VTEX estão estabelecidos no Anexo 1B deste DPA.

Local, data e assinaturas na Proposta Comercial

Este DPA é celebrado e se torna uma parte indissociável do Contrato a partir da Data de Vigência do DPA.

ANEXO 1 - DESCRIÇÃO DO TRATAMENTO

1A. LISTA DE PARTES E SUB-OPERADORES

Todas as partes encontram-se em nosso site:
https://vtex.com/us-en/privacy-and-agreements/subprocessors/

O controlador autorizou o uso dos seguintes operadores e sub- operadores:

1. **Controlador para Operador**

    a. **Exportador de dados: CONTRATANTE IDENTIFICADA NO MASTER SERVICE AGREEMENT.**
    Função (controlador/operador): Controlador

    b. **Importador de dados: VTEX BRAZIL**
    Nome: VTEX Brasil Tecnologia para E-commerce LTDA
    Endereço: Avenida Brigadeiro Faria Lima, nº 4.440, 10º andar, Vila Olímpia, CEP 04538-132, inscrita no CNPJ/MF sob o n. 05.314.972/0001-74
    Função (controlador/operador): Operador

    c. **Importador de dados: AWS**
    Nome: Amazon Web Services Inc.
    Endereço: Estados Unidos
    Função (controlador/operador): Sub-operador

1B. DESCRIÇÃO DO TRATAMENTO

Objeto e duração do tratamento dos Dados Pessoais.

O objeto do Tratamento dos Dados Pessoais da Contratante é conforme estabelecido no Contrato e neste DPA. As operações de Tratamento são realizadas no contexto do Contrato, e na gestão dos Serviços prestados pela VTEX à Contratante.

A duração do Processamento coincide com a vigência do Contrato.

Natureza do tratamento, finalidade(s) da transferência de dados e tratamento adicional

Os Dados Pessoais transferidos serão tratados para fins de execução dos Serviços nos termos do Contrato e da qualquer Proposta Comercial, sujeitos às seguintes atividades de tratamento:

- armazenamento e outras modalidades de tratamento necessárias para fornecer, manter e atualizar os Serviços prestados ao Contratado;
- manutenção e suporte técnico da Contratante; e
- divulgações de acordo com o Contrato, conforme exigido por lei.

Não há tratamento adicional além de transferências para sub-operadores.

Categorias de Titulares de Dados existentes nos Dados Pessoais da Contratante

As categorias de Titular dos Dados podem incluir alguns ou todos dentre os seguintes:

- Colaboradores da Contratante;
- Usuários finais da Contratante (clientes)

Espécies de Dados Pessoais: Endereço IP; informações de navegação como cookies; informações do carrinho; informações do pedido; email; número de telefone; endereço de entrega; número de identidade, histórico do cartão-presente; nome; histórico de pedidos; informações de navegação; carrinho não utilizado; conversas; senhas de sessões; tokens gerados; sessões.

Dados pessoais sensíveis transferidos (se aplicável): restrições ou salvaguardas aplicadas que levem em consideração a natureza dos dados e os riscos envolvidos, como, por exemplo, finalidade estrita, restrições de acesso (incluindo acesso apenas para funcionários que seguiram treinamento especializado), manutenção de um registro de acesso aos dados, restrições para transferências posteriores ou medidas de segurança adicionais. Os Exportadores de Dados podem enviar Dados Pessoais Sensíveis ao Importador de Dados, conforme o caso, por meio dos Serviços, cuja extensão é determinada e controlada pelo Exportador de Dados em conformidade com as Leis de Proteção de Dados.

Obrigações e direitos da Contratante e da VTEX.

As obrigações e direitos da Contratante e da VTEX estão estabelecidos no Contrato e neste DPA.

Frequência da transferência (por exemplo, se os dados são transferidos de forma pontual ou contínua).

Os dados são transferidos de forma contínua para fins dos Serviços a serem prestados nos termos o Contrato e qualquer Formulário de Pedido - Proposta Comercial.

O período de retenção dos dados pessoais ou, se isso não for possível, os critérios usados para determinar esse período

A ser mutuamente acordado entre a Contratante e a VTEX, de acordo com as leis aplicáveis ao Controlador que regem a privacidade, transações de comércio eletrônico e leis tributárias.

Para transferências para (sub) operadores, especifique o objeto, a natureza e a duração do tratamento

A VTEX contrata a Amazon Web Services Inc. e a Microsoft Inc. (Azure) como Provedores de Serviços em Nuvem para fins de hospedagem, pela duração do Master Services Agreement celebrado entre a VTEX e a Contratante.

ANEXO 2

MEDIDAS TÉCNICAS E ORGANIZACIONAIS PARA GARANTIR A SEGURANÇA DOS DADOS

A VTEX implementou e compromete-se a manter medidas técnicas e organizacionais apropriadas para proteger os dados pessoais contra uso indevido e perda ou destruição acidental conforme suas Políticas de Privacidade e Segurança.

As medidas técnicas e organizacionais atuais da VTEX estão descritas abaixo e no ambiente admin da Contratante, no qual haverá uma versão atualizada regularmente.

Segue abaixo uma lista não exaustiva de pontos que estão atualmente implementados na VTEX com foco em proteção e segurança de dados considerando a tríade: TI, Segurança e Privacidade.

1. Conscientização e Treinamento
    a. A VTEX possui ciclos de treinamento para diferentes níveis de funcionários com foco em privacidade e segurança. A VTEX também terá treinamento focado em boas práticas em desenvolvimento seguro.
2. Proteção de senhas
    a. A VTEX atualmente armazena as senhas de uma maneira: HashVector (o algoritmo principal usado é PBKDF2 com SHA256).
3. Política antivírus
    a. A equipe de TI tem como política manter todos os computadores de seu grupo com antivírus.
4. Classificação de Informações
    a. VTEX possui uma política de classificação de informações para entender que tipo de proteção é adequada ao tipo de dado.
5. Gerenciamento de Vulnerabilidades
    a. A VTEX realiza análises regulares de ameaças e vulnerabilidades da plataforma e dos processos operacionais. A identificação de riscos desencadeia a melhoria dos nossos sistemas de monitoramento e notificação para lidar com eventuais concretização de tais riscos, seja por meio da notificação aos colaboradores que possam lidar com eles, seja através do desencadeamento de ações automatizadas para mitigá-los ou eliminá-los. No ponto 15 do anexo trazemos detalhadamente o funcionamento de nossos *pentests*.
6. Certificações
    a. Conforme definido pelos padrões de indústria, as certificações normalmente cobrem um período de janeiro a dezembro; sendo dezembro o mês para renovar a certificação para o ano corrente. Assim, quando falamos das certificações atuais, estamos nos referindo àquelas que mantivemos até o período mais recente. As certificações que a VTEX manteve até o período mais recente, portanto, são:

        i. SOC 1 - Tipo 2: relatório que compreende os controles internos sobre os sistemas de relatórios financeiros;
        ii. SOC 2 - Tipo 2: relatório que compreende Segurança, Disponibilidade, Integridade, Confidencialidade e Privacidade;
        iii. SOC 3: relatório público de Segurança, Disponibilidade, Integridade, Confidencialidade e Controles de Privacidade;
        iv. PCI: validação dos controles em dados do titular do cartão, a fim de reduzir fraudes no cartão de crédito.
        v. Todas essas certificações estão disponíveis na seção Compliance no VTEX Trust Hub (https://vtex.com/us-en/trust/)

7. Medidas da VTEX para garantir a segurança dos dados
    a. Os dados em trânsito são sempre criptografados, além disso a VTEX possui soluções internas para construção de segurança de aplicativos, e também realiza ciclos de testes com empresas terceirizadas para aprimorar soluções; além do uso de políticas de backup e avaliação de possíveis falhas e revisões de incidentes. Por fim, as auditorias externas garantem que a maioria desses fluxos: anonimização de dados, tratamento seguro, dentre outros, sejam respeitados e cumpridos.
8. Como abordamos o Backup e a Redundância de Dados
    a. A maioria dos dados tratados pela VTEX é armazenada em serviços da AWS usando serviços gerenciados como S3, RDS e DynamoDB. Todos esses serviços fornecem infraestrutura de backup gerenciada pela AWS, que é utilizada pela VTEX. A plataforma AWS é referência no setor de computação em nuvem e possui importantes certificações como: ISO 27001, PCI DSS, CSA, NIST, dentre outras. (Para ver uma lista detalhada de certificações, acesse: https://aws.amazon.com/en/compliance/programs/).
9. Recuperação de desastres e recuperação de incidentes
    a. O Plano de Recuperação de Desastres e Incidentes da VTEX consiste em políticas e procedimentos internos que a VTEX seguirá em caso de interrupção do serviço. Isso pode acontecer por causa de um desastre natural, ou como resultado de falhas tecnológicas ou fatores humanos. O objetivo é restaurar os processos de negócios afetados o mais rápido possível, seja colocando os serviços interrompidos novamente online, ou transicionando para um sistema de contingência.
    b. O escopo do plano é a VTEX Cloud Commerce Platform, incluindo: (i) todos os serviços que constituem a solução; (ii) todos os processos internos que o suportam ou a sua operação; (iii) todos os processos de negócios que dão suporte aos Contratantes da VTEX que dependem da VTEX Cloud Commerce Platform.
    c. O Plano de Recuperação de Desastres e Incidentes da VTEX é totalmente suportado e implementado por processos automatizados que são acionados com base em ferramentas também automatizadas de monitoramento e notificação.
    d. Objetivo de Tempo de Recuperação (RTO): é o prazo máximo que deve decorrer antes que os serviços normais sejam retomados. O tempo de inatividade do serviço pode estar relacionado à interrupção do aplicativo, corrupção ou perda de dados, falha do servidor de dados ou interrupção da zona ou região de disponibilidade da AWS. O Plano de Recuperação de Desastres e Incidentes da VTEX é testado pelo menos uma vez por ano, a fim de verificar se será eficaz no momento em que for necessário.
    e. As partes interessadas são notificadas através da página de status (https://status.vtex.com): a página de status está disponível publicamente para qualquer pessoa interessada em ver o status de integridade atual da plataforma VTEX True Cloud CommerceTM. Também é utilizado como ferramenta de notificação para manutenção planejada, que não está no escopo do Plano de Recuperação de Desastres.
10. Criptografia de dados privados
    a. Seguindo nosso compromisso com a conformidade com a LGPD, a VTEX garante a criptografia de acordo com o que os regulamentos de privacidade e conformidade em torno dos dados pessoais. Nosso Produto de Pagamentos é compatível com PCI e implementa criptografia de dados e rotação de chaves de acordo com os padrões PCI DSS. Além disso, a VTEX tem projetos de engenharia em andamento para implementar criptografia e isolamento de dados pessoais, bem como implementar registro de auditoria em diversos aplicativos.
11. Armazenamento de dados VTEX
    a. O provedor de hospedagem da VTEX é a AWS, líder mundial no fornecimento de serviços de computação em nuvem, e os dados são armazenados na região AWS do estado da Virgínia, Estados Unidos. Um dos principais pilares da AWS é “Segurança

é Job Zero", uma afirmação que comprova que a segurança da informação é colocada antes de tudo na AWS, e com a qual a VTEX se identifica.

12. Transmissão de Dados
    a. Todo o tráfego de entrada na rede da VTEX é protegido usando a tecnologia TLS 1.2 sobre http.
13. Segregação de clientes e redes
    a. A rede de produção é completamente isolada das redes externas. Os funcionários da VTEX responsáveis pela operação dos ambientes de produção podem precisar de eventual conexão VPN para acessar a rede de produção.
14. Medidas de físicas de segurança
    a. Os ativos físicos utilizados pela VTEX são fornecidos pela AWS como parte do serviço prestado por eles.
15. Políticas de pentest
    a. Devido à natureza do negócio da VTEX, estamos construindo uma política de realizar pentests trimestralmente. Atualmente os testes ocorrem anualmente. Além disso, vários clientes avaliam nossa plataforma de forma independente, por isso somos sempre auditados externa e internamente.
16. Controles para sub-operadores

    a. A VTEX possui um questionário de análise de sub-operadores que inclui perguntas de segurança para analisar os riscos potenciais. Os métodos utilizados para avaliar a segurança de terceiros são escolhidos considerando o tipo e gravidade dos riscos nessas relações, a adequação e relevância dos detalhes sobre processos e controles de segurança. Mais especificamente, a AWS, listada como sub-operador no Anexo 1, possui as certificações de segurança e privacidade ISO 27017:2015 e ISO 27018:2014, que são subconjuntos baseados na ISO 27001:2013, o padrão de segurança mais abrangente.

***