VTEX Global Data Processing Addendum

Esse **Data Processing Addendum** da VTEX (**"DPA"**) serve como Apêndice 2 ao Master Service Agreement ("MSA") disponível em https://vtex.com/us-en/Contratos, assinado pelo Cliente e pela VTEX. Juntos, o Master Services Agreement ("MSA"), o Order Form - Commercial Proposal e este DPA, são chamados de "**Contrato**".

Em consideração às premissas mútuas estabelecidas neste DPA, o Cliente e a VTEX concordam que:

1 Tipos de Dados & Finalidades de Tratamento

Delineados abaixo estão os tipos de dados pessoais, categorias de Titulares, finalidades, e pontos e métodos de coleta de dados pessoais que serão tratados. .

Dados pessoais	*Identificadores pessoais:* - Nome e/ou sobrenome, pseudônimo, assinatura, email, endereço ou telefone - Documento de identificação governamental (ex.: CPF, CNPJ, RUT, número de passaporte, número da carteira de habilitação) *Informações de pagamento:* - Número do cartão de crédito ou débito (encriptados conforme padrões do PCI-DSS) *Dados gerados online:* - Identificador pessoal único ou identificador eletrônico (ex.: cookies ou endereço de IP) - Informações de acesso (ex.: username e/ou senha encriptada) - Informações de atividade (ex.: histórico de navegação, histórico de busca, informações do carrinho, histórico de pedidos, histórico de gift cards, histórico de contato com suporte, ou interações com conteúdo e anúncios) - Inferências derivadas de preferências e comportamento
A quem os dados pertencem (Categorias de Titulares)	- Consumidores finais do Cliente (ex.: shoppers ou compradores, visitantes do site, ou inscritos) - Empregados do Cliente
Finalidades para o tratamento de dados	- Serviços de Performance sob o Contrato (ex.: manutenção ou fornecimento de contas, provimento de serviços ao Cliente, cumprimento de pedidos e transações, processamento de pagamentos, provimento de serviços de anúncio ou marketing conforme instruções do Cliente) - Auditoria relacionada a uma interação atual (por exemplo, contagem e verificação de impressões de anúncios) - Detectar, prevenir e investigar incidentes de segurança, atividades fraudulentas ou ilegais - Depurar erros que prejudicam a funcionalidade e manter ou melhorar a disponibilidade dos Serviços - Melhoria e desenvolvimento de produtos - Realizar análise, agregação e/ou desidentificação de dados, inclusive para desenvolver insights em benefício de Cliente
Ponto de coleta de dados	- Site, aplicativo móvel ou serviço digital semelhante do Cliente

Método de coleta de dados	- Formulários preenchidos diretamente pelo Titular (por exemplo, inscrição em newsletter, pesquisa, formulário de inscrição) - Cookies, pixels, tags, SDKs e tecnologias semelhantes

2 Definições e Interpretação.

Quaisquer termos em letras maiusculas são definidos: (i) nas **Leis de proteção de dados** aplicáveis, como "**Controlador de Dados**", "**dados pessoais**", "**Operador de Dados**" e "**Sub-operador**"; (ii) pelos significados que lhes são atribuídos no MSA; ou (iii) nesta cláusula. Para os fins deste DPA, "**dados pessoais**" significa qualquer informação relacionada a uma pessoa física identificada ou identificável, protegida pelas Leis de Proteção de Dados aplicáveis, fornecida pelo Cliente, na posição de Controlador de Dados, à VTEX, na posição de Operador de Dados, no contexto do desempenho de o Contrato.

"**Afiliado**" significa qualquer entidade que direta ou indiretamente controle, seja controlada ou esteja sob controle comum do Cliente. "Controle", para fins desta definição, significa propriedade ou controle direto ou indireto de mais de 50% dos interesses com direito a voto da entidade em questão.

"**Usuários Autorizados**" significa qualquer pessoa a quem o Cliente tenha concedido acesso ao ambiente da Plataforma VTEX de acordo com os requisitos estabelecidos no Contrato.

"**Cliente**" significa a entidade identificada no *Order Form - Commercial Proposal* que assina este DPA em seu nome e em nome de quaisquer Afiliadas do Cliente.

"**Afiliado do cliente**" significa qualquer Afiliado(s) do Cliente que tenha permissão para usar os Serviços de acordo com o MSA entre o Cliente e a VTEX. Se e na medida em que a VTEX tratar dados pessoais em nome de tal(s) Afiliado(s), o Afiliado se qualificará como Controlador.

"**Dados pessoais do Cliente**" significa quaisquer dados pessoais relativos aos Usuários Autorizados recebidos para fins de autorização de acesso aos Serviços, ou aos representantes do Cliente ou Afiliadas em conexão com a execução e administração do Contrato, cujos dados pessoais a VTEX trata como controladora.

"**DPF**" significa os mecanismos de transferência de dados pessoais para os Estados Unidos da União Europeia/Espaço Económico Europeu, do Reino Unido (e de Gibraltar) e da Suíça, de acordo com o *EU-U.S. Data Privacy Framework* ("**EU-U.S. DPF**"), com o *UK Extension to the EU-U.S. Data Privacy Framework* ("**UK Extension to the EU-U.S. DPF**"), e com o *Swiss-U.S. Data Privacy Framework* ("**Swiss-U.S. DPF**"), com base na decisão de adequação da Comissão Europeia em vigor em 10 de julho de 2023.

"Leis de Proteção de Dados" significa todas as leis, regulamentos por autoridades supervisoras de proteção de dados e ordens judiciais/administrativas em qualquer jurisdição ao qual o Cliente está vinculado em conexão com os Serviços prestados nos termos do Contrato, incluindo aquelas relativas a: (a) privacidade; (b) a segurança, perda ou uso indevido de dados, (c) marketing e anúncios comerciais; e (d) uso responsável e proteção de dados.

"SCC" significa as seções I, II, III e IV (conforme aplicável) na medida em que fazem referência ao Módulo Dois (Controlador para Operador) dentro das Cláusulas Contratuais Padrão (ou *Standard Contractual Clauses*) para a transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho aprovado pela Decisão de Execução (UE) 2021/914 da Comissão Europeia, de 4 de junho de 2021, conforme atualmente estabelecido em https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, conforme alterado, substituído ou é necessário que seja implementado em conexão com o SCC de vez em quando.

"**SCC do Reino Unido**" significa o SCC transposto para a legislação nacional do Reino Unido por operação da seção 3 da Lei da União Europeia (Retirada) de 2018 e conforme alterado pelos Regulamentos de Proteção de Dados, Privacidade e Comunicações Eletrônicas (Emendas etc.) (Saída da UE) de 2019 ("**GDPR do Reino Unido**"), de acordo com o Artigo 46 do GDPR do Reino Unido.

"Violação de segurança" significa o acesso, perda, alteração ou divulgação acidental ou não autorizada de dados pessoais tratados. Uma Violação de Segurança inclui, sem limitação, um "vazamento de dados pessoais" ou outro termo semelhante conforme definido nas Leis de Proteção de Dados.

"**Autoridade Supervisora**" significa uma autoridade reguladora independente responsável pela aplicação das leis de proteção de dados.

3 Detalhes de tratamento.

3.1 **Papeis das Partes.** Para efeitos deste DPA, o Controlador de Dados é o Cliente (conforme definido no Order Form - Commercial Proposal) e qualquer Afiliada do Cliente; o Operador de Dados é a VTEX (conforme definido no Order Form - Commercial Proposal); e os Sub-operadores são AWS (Northern Virginia Region - USA) and VTEX Brasil Tecnologia para E-commerce Ltda.

3.2 **Transferências Internacionais de Dados**. Quando a VTEX tratar dados pessoais de Titulares localizados na Área Econômica Europeia, na Suíça ou no Reino Unido em um país que não tenha recebido uma decisão de adequação da Comissão Europeia ou de autoridades suíças ou do Reino Unido, conforme aplicável, tal transferência ocorrerá com base em Certificação da VTEX no DPF. Se o DPF for declarado inválido, ou se a VTEX não conseguir recertificar-se no DPF, então a transferência de dados pessoais estará sujeita ao SCC ou UK SCC, conforme aplicável, que as partes concordam que será incorporado por referência a este DPA. As partes concordam que, no que diz respeito aos elementos das SCCs e da SCC do Reino Unido que exigem a contribuição das partes, os Schedules 1-4 contêm todas as informações relevantes.

3.3 **Escopo do Processamento.** O Contrato contém as instruções completas e finais do Cliente no momento da execução do DPA para o Tratamento de dados pessoais. Quaisquer instruções adicionais ou alternativas deverão ser solicitadas separadamente por escrito à VTEX. VTEX deverá sempre: (i) tratar dados pessoais apenas com a finalidade de fornecer os Serviços a Cliente conforme descrito na tabela nas páginas 1 e 2 e Schedules 1-4 para efeitos do SCC; (ii) de acordo com instruções documentadas do Cliente; e (iii) não tratar dados pessoais para seus próprios fins ou de terceiros. VTEX notificará imediatamente Cliente por escrito, a menos que seja proibido de fazê-lo sob as Leis de Proteção de Dados ou outras leis aplicáveis, se: (a) tomar conhecimento ou acreditar que qualquer instrução de tratamento de dados da Cliente viola as Leis de Proteção de Dados ou não consegue cumprir as instruções de tratamento de dados do Cliente; e/ou (b) não for capaz de cumprir os termos do Contrato na medida em que se relacionam ou regem o tratamento e/ou a segurança de dados pessoais.

3.4 **Obrigações Mútuas.** Na medida aplicável ao desempenho ou uso dos Serviços por cada parte, conforme o caso, inclusive na medida em que cada parte coleta dados pessoais diretamente de indivíduos, cada parte declara e garante que irá: (i) cumprir as Leis de Proteção de Dados com relação a quaisquer dados pessoais recebidos, coletados, tratados, compartilhados ou armazenados por tal parte, incluindo quaisquer diretrizes, estruturas ou códigos autorregulatórios aplicáveis do setor; (ii) manter avisos de privacidade, divulgações de cookies e/ou outras declarações legalmente exigidas, visíveis ao consumidor, que divulguem com precisão todas as práticas aplicáveis de coleta, uso, compartilhamento, divulgação e segurança de dados; (iii) obter quaisquer permissões necessárias e consentimentos de adesão ou exclusão de indivíduos e respeitar essas escolhas do consumidor; (4) estabelecer e manter processos legais para o exercício de direitos dos Titulares e

honrar quaisquer solicitações de direitos válidas relacionadas dados pessoais e dados pessoais do Cliente, como aplicável a cada parte; e (v) garantir que os indivíduos com acesso a dados pessoais estejam sujeitos a uma obrigação contratual ou estatutária adequada de confidencialidade.

4 Obrigações do Cliente.

4.1 **Base legal**. O Cliente é o único responsável pela exatidão, qualidade e licitude dos dados pessoais e pelos meios pelos quais o Cliente adquiriu os dados pessoais fornecidos à VTEX. O Cliente garante que possui uma base legal para compartilhar os dados pessoais com a VTEX e para que a VTEX trate os dados pessoais conforme previsto no Contrato.

5 Obrigações da VTEX.

5.1 **Schedules Regionais.** VTEX concorda em incluir obrigações adicionais de acordo com as leis em vigor no país e/ou território aplicável a Cliente, conforme estabelecido no Order Form. Tais obrigações estão previstas no CCPA Schedule, LATAM Schedule, GDPR Schedule, e outros Schedules, cada um na medida aplicável ao tratamento de dados pessoais realizado pela VTEX de acordo com a lei aplicável e territórios estabelecidos na MSA. Na medida em que haja quaisquer conflitos entre um Schedule e o corpo principal deste DPA, o Schedule prevalecerá.

5.2 **Direitos do Titular e Cooperação.**

5.2.1 VTEX cooperará com o Cliente para habilitar o Cliente a responder a quaisquer solicitações, reclamações ou outras comunicações válidas de indivíduos, órgãos reguladores ou judiciais, ou outras entidades relevantes, relacionadas ao tratamento de dados pessoais (**"Solicitação"**), incluindo Solicitações de indivíduos para exercerem seus direitos sob as Leis de Proteção de Dados. Caso tal Solicitação seja feita diretamente a VTEX, VTEX deverá notificar o cliente por escrito dentro 2 (dois) dias úteis.

5.2.2 Se VTEX receber uma intimação, ordem judicial, mandado ou outra exigência legal de terceiros (incluindo autoridades policiais ou outros serviços públicos ou de proteção de dados). autoridades de supervisão) buscando a divulgação de dados pessoais, na medida em que não seja proibido por lei, VTEX notificará imediatamente Cliente por escrito de tal solicitação, e cooperar razoavelmente com Cliente se este desejar limitar, contestar ou proteger contra tal divulgação.

5.3 **Sub-operadores e Funcionários.** Cliente reconhece e concorda que (a) as Afiliadas da VTEX são Sub-operadores sob este DPA especialmente para fins de suporte técnico e (b) a VTEX e as Afiliadas da VTEX podem contratar Sub-operadores terceirizados, como AWS, Região da Virgínia Norte, EUA, em conexão com a prestação dos Serviços. Uma lista atualizada dos Suboperadores contratados pela VTEX para a prestação dos Serviços está disponível em https://vtex.com/us-pt/privacy-and-Contratos/Sub-operadores/ ("**Lista de Sub-operadores**"). A VTEX imporá contratualmente o mesmo nível de proteção ou superior aos Sub-operadores para tratamento de dados pessoais conforme previsto neste DPA. A VTEX deverá garantir que funcionários autorizados a tratar dados pessoais sejam: (i) obrigados a manter dados pessoais confidenciais; e (ii) devidamente treinados no tratamento de dados pessoais sob as Leis de Proteção de Dados aplicáveis.

5.4 **Avaliação de impacto na proteção de dados.** Na medida que o Cliente de outra forma não tiver acesso às informações relevantes, a VTEX fornecerá ao Cliente com cooperação e assistência razoáveis necessárias para realizar uma avaliação de impacto à proteção de dados, ou qualquer avaliação semelhante exigida pelas Leis de Proteção de Dados, relacionada ao uso dos Serviços por parte do Cliente, quando um tipo de tratamento pode resultar em um alto risco para os direitos e liberdades das pessoas físicas.

5.5 **Medidas de segurança e auditorias de conformidade.**

5.5.1 VTEX irá: (i) implementar medidas de segurança técnicas e organizacionais apropriadas para proteger dados pessoais de uma Violação de Segurança usando medidas apropriadas aos riscos apresentados pela natureza do tratamento de dados pessoais (e tais medidas atenderão ou excederão aquelas identificadas no Schedule 3); (ii) monitorar regularmente o cumprimento de tais medidas; (iii) mediante solicitação, disponibilizar ao Cliente uma cópia de sua auditoria de terceiros mais recente resultados ou certificações relacionadas a tais medidas, na medida em que VTEX torna-os geralmente disponíveis aos seus clientes; e (iv) responder oportunamente às solicitações anuais do Cliente em relação ao questionário de segurança e privacidade da informação da VTEX. Se, na determinação razoável do Cliente, as informações fornecidas em (iii) e (iv) forem inadequadas ou no caso de uma Violação de Segurança, VTEX concorda em permitir uma auditoria ou inspeção independente de terceiros (desde que tal auditoria ou inspeção seja realizada por um auditor mutuamente acordado entre as partes, às custas exclusivas do Cliente e não mais do que uma vez por ano exceto se a auditoria ou inspeção ocorrer em resposta a uma Violação de Segurança). Antes do início de qualquer auditoria ou inspeção independente, o Cliente e a VTEX concordarão mutuamente sobre o escopo, o momento e a duração da auditoria ou inspeção e a VTEX fornecerá assistência e cooperação razoáveis para permitir tal auditoria ou inspeção. Quando exigido pelas Leis de Proteção de Dados, a VTEX manterá um plano e/ou política por escrito abrangente relacionado à implementação de tais medidas e fornecerá um resumo de tal plano e/ou política ao Cliente, mediante solicitação.

5.5.2 **Auditorias.** O Cliente poderá auditar o cumprimento, pela VTEX, das Medidas Técnicas e Organizacionais relevantes aos dados pessoais tratados pela VTEX ("**Auditoria de Cliente**") mediante solicitação e somente se:

(a) a VTEX não forneceu evidências suficientes de sua conformidade com as Medidas Técnicas e Organizacionais estabelecidas no Schedule 3, 3.3, por exemplo, ISO 27001, SOC 2 - Tipo 2, ou outras normas definidas nas certificações ("**Relatórios de Auditoria e Certificações**"); ou

(b) ocorreu uma violação de dados pessoais; ou

(c) uma auditoria for formalmente solicitada pela autoridade de proteção de dados do Cliente; ou

(d) u,a Lei de Proteção de Dados estabelece um direito de auditoria direta.

5.5.3 **Especificações de auditoria.** Antes de iniciar uma solicitação de auditoria, o Cliente analisará os Relatórios de Auditoria e Certificações da VTEX. O Cliente ou seu auditor terceirizado independente (razoavelmente aceitável pela VTEX, agindo em nome do Cliente) deverá fornecer aviso prévio com pelo menos 60 (sessenta) dias de antecedência sobre qualquer Auditoria do Cliente, a menos que uma Lei de Proteção de Dados ou uma autoridade de proteção de dados do Cliente exija um aviso mais curto. A data de início, o prazo e o escopo de qualquer Auditoria do Cliente serão mutuamente acordados entre as partes, agindo de forma razoável. A menos que as Leis de Proteção de Dados exijam auditorias mais frequentes, a frequência de uma Auditoria do Cliente não deverá exceder uma vez a cada 12 meses. Os recursos da VTEX para apoio às Auditorias de Clientes serão limitados a um máximo equivalente a 3 (três) dias úteis, durante o horário comercial normal da VTEX, não perturbarão as operações normais de negócios da VTEX e estarão sujeitos aos requisitos de confidencialidade da VTEX. O Cliente compartilhará qualquer relatório resultante de uma Auditoria de Cliente para a VTEX.

5.5.4 **Custos de auditoria**. Caso uma auditoria seja conduzida fora das especificações fornecidas em 5.5.3, então o Cliente cobrirá todos os custos razoáveis de tal auditoria e qualquer trabalho exigido da VTEX, de acordo com as taxas então vigentes da VTEX. Se a Auditoria do Cliente revelar uma violação material deste DPA por parte da VTEX, então a VTEX realizará sua própria auditoria, para confirmar tal violação material. Nesse caso, serão aplicados os procedimentos de remediação estabelecidos no Contrato.

5.6 **Violação de segurança.**

5.6.1 No caso de uma Violação de Segurança, a VTEX vai:

(i) Prontamente, e em nenhum caso depois 72 (setenta e duas) horas após tomar conhecimento de tal Violação de Segurança, informar o Cliente e fornecer detalhes por escrito da Violação de Segurança, incluindo, se aplicável, os tipos de dados pessoais afetados e a identidade da(s) pessoa(s) impactada(s) assim que tal informação se tornar conhecida ou disponível para VTEX;

(ii) Fornecer informações oportunas e cooperação conforme o Cliente pode exigir para o cumprimento de suas obrigações de comunicação de violação de dados de acordo com as Leis de Proteção de Dados ou o cumprimento ou resposta a quaisquer consultas de uma autoridade de proteção de dados ou qualquer ação judicial decorrente da Violação de Segurança, exceto quando tais informações incluem informações confidenciais de terceiros;

(iii) Investigar a Violação de Segurança e realize uma análise de causa;

(iv) Tomar as medidas e ações apropriadas para remediar ou mitigar os efeitos da Violação de Segurança e manter Cliente atualizado sobre os desenvolvimentos relacionados à Violação de Segurança; e

(v) Caso a análise da causa demonstre que a Violação de Segurança foi causada exclusivamente pela VTEX, a VTEX reembolsará o Cliente por quaisquer custos e despesas razoáveis incorridos em conexão com uma Violação de Segurança, incluindo o custo de notificações a indivíduos e serviços de monitoramento e resolução de roubo de identidade (incluindo serviços de monitoramento de crédito) às partes afetadas, nos termos da cláusula 6. Responsabilidade.

5.6.2 O conteúdo e o fornecimento de qualquer notificação, comunicação pública/regulatória ou comunicado de imprensa relativo à Violação de Segurança serão exclusivamente do Cliente, exceto se exigido de outra forma pelas Leis de Proteção de Dados ou se houver referência à VTEX em tais anúncios – nesse caso, a VTEX deverá aprovar o conteúdo por escrito e previamente para qualquer anúncio.

5.7 **Exclusão e/ou transferência**. A VTEX irá, a qualquer momento, mas não após a rescisão do Contrato, fornecer os meios para que o Cliente extraia uma cópia completa de todos os dados pessoais em posse da VTEX ou, na ausência de quaisquer instruções do Cliente, destruirá com segurança tais dados pessoais. O Cliente reconhece que a VTEX poderá cumprir a obrigação acima, fornecendo as interfaces necessárias para que o Cliente recupere os dados pessoais por meios próprios, no próprio ambiente administrativo do Cliente na Plataforma VTEX. Esta opção permanecerá disponível, por padrão, até a data de rescisão do Contrato.

6 Responsabilidade.

6.1. A responsabilidade de cada parte e de todas as suas Afiliadas, tomadas em conjunto no agregado, decorrente ou relacionada a este DPA, e todos os DPAs entre Cliente e as Afiliadas e a VTEX, seja por contrato, ato ilícito ou sob qualquer outra teoria de responsabilidade, estão sujeitas à seção "**LIMITAÇÃO DE RESPONSABILIDADE DA VTEX**" do MSA. Qualquer referência nessa seção à responsabilidade de uma parte significa a responsabilidade agregada dessa parte e de todas as suas Afiliadas nos termos da MSA. Em particular, o conjunto de todas as reivindicações não deve ser entendido como aplicável individual e solidariamente a Cliente e/ou para qualquer Afiliada que é parte contratual da MSA. A VTEX será responsável pelos atos e omissões de seus Sub-operadores na mesma medida que a VTEX seria responsável se prestasse os serviços de cada Sub-operador diretamente nos termos deste DPA.

7 Lei Aplicável e Resolução de Disputas

Conforme estabelecido na Cláusula "**LEI APLICÁVEL E ARBITRAGEM**" no MSA.

Como exceção ao acima exposto, apenas em relação às transferências restritas do Reino Unido, a "**legislação aplicável**" será a lei da Inglaterra e do País de Gales.

Local, data e assinaturas no Order Form - Commercial Proposal

CONSIDERANDO QUE, este DPA é celebrado e se torna uma parte vinculativa do Contrato.

Schedule 1: Transferências Internacionais - Descrição do Processamento e Sub-operadores

Atividade de tratamento	**Cliente divulga dados pessoais do Cliente à VTEX para fornecer, operar e manter os Serviços VTEX**	**Cliente contata a VTEX para suporte técnico**	**Cliente trata dados pessoais de usuários-finais / dados pessoais de shoppers nos Serviços VTEX**
Tipos de dados e finalidades de tratamento	Consulte "Tipos de dados e finalidades de tratamento" no DPA.		
Situação das Partes	VTEX e Cliente são Controladores de Dados	VTEX e Cliente são Controladores de Dados	VTEX é Operador de Dados Cliente é Controlador de Dados
Categorias de dados pessoais tratados	Registro de conta, conteúdo do usuário, comunicação, tecnologias de rastreamento, uso de Serviços e contas de terceiros (de acordo com integrações escolhidas pelo Cliente).	Registro de conta, conteúdo do usuário, comunicações, uso de Serviços e contas de terceiros (de acordo com integrações escolhidas pelo Cliente).	Conforme determinado pelo Cliente (consulte a seção "Tipos de dados e finalidades de tratamento" no DPA).
Categories of Sensitive dados pessoais Processed	Nenhum	Nenhum	Conforme determinado pelo Cliente
Frequência de Transferência	Contínuo	Contínuo	Conforme determinado pelo Cliente
Módulo SCC aplicável	Módulo 1	Módulo 1	Módulo 2
Sub-operadores	Para uma lista completa, consulte https://vtex.com/us-pt/privacy-and-Contratos/Sub-operadores/ **Exportador de dados:** Cliente nomeado no Contrato **Importador de dados:** Entidade VTEX indicada no Contrato **Sub-operador 1**: VTEX Brasil Tecnologia para E-commerce Ltda. para fins de suporte técnico **Sub-operador 2**: Amazon Web Services Inc., Região da Virgínia Norte, EUA.		

Schedule 2: Informações para SCC - Módulo 1

1. Períodos de retenção

A VTEX retém os dados pessoais que coleta como Controlador enquanto a VTEX tiver um propósito comercial para isso ou pelo maior período permitido pela legislação aplicável.

2. SCC

2.1. Para fins das Cláusulas Contratuais Padrão:

Cláusula 7, Módulo 1: As partes concordam que a cláusula de docagem (*docking clause*) não será aplicável.
Cláusula 11(a), Módulo 1: As partes não selecionam a opção de resolução independente de disputas.
Cláusula 17, Módulo 1: As partes selecionam a Opção 1. O Estado Membro é o indicado na cláusula de foro do Contrato.
Cláusula 18(b), Módulo 1: As Partes concordam que esses serão os tribunais conforme indicado na cláusula de foro do Contrato.

Anexo I (A): O exportador de dados é o Cliente. O importador de dados é a VTEX. Os detalhes de contato do Cliente são os endereços de e-mail designados pelo Cliente na conta VTEX do Cliente. O contato da VTEX é dpo@vtex.com, ou conforme declarado no Contrato.

Anexo I (B): As partes concordam que o Schedule 1 descreve a transferência.

Anexo I (C): A autoridade de supervisão competente é a autoridade supervisora do ICO.

Anexo II: As Partes concordam que o Schedule 3, Seção 3.3. descreve as medidas técnicas e organizacionais aplicáveis à transferência.

2.2. Para fins do Adendo do Reino Unido:

Tabela 1: O exportador de dados é o Cliente. O importador dos dados é a Entidade VTEX indicada no Contrato. Os detalhes de contato do Cliente são os endereços de e-mail designados pelo Cliente na conta VTEX do Cliente. O contato da VTEX é dpo@vtex.com, ou conforme declarado no Contrato.

Tabela 2: As Partes marcam a caixa de seleção que diz: “SCCs da UE aprovadas, incluindo as Informações do Apêndice e apenas com os seguintes módulos, cláusulas ou disposições opcionais das SCCs da UE aprovadas em vigor para os fins deste Adendo”, e a tabela anexa será considerada concluída de acordo com as preferências das Partes descritas no Schedule 2, Seção 2.1 acima.

Tabela 3: A Tabela 3 deverá ser preenchida com as informações estabelecidas no Schedule 2, Seção 2.1 acima, referente ao Anexo I(A), Anexo I(B) e Anexo II.

Tabela 4: As Partes concordam que o importador de dados pode rescindir o Adendo do Reino Unido, conforme estabelecido na Seção 19 do Adendo do Reino Unido.

IDTA do Reino Unido será adicionado

Tabela 1: Consulte o Contrato.

Tabela 2: Lei do país do Reino Unido que rege o IDTA e local principal para reivindicações legais a serem feitas pelas Partes: Inglaterra e País de Gales. Status do Exportador e do Importador: Consulte o Schedule 1. Se o GDPR do Reino Unido se aplica ao Importador: Consulte o Contrato. Contrato e Prazo Vinculados: Consulte o Contrato. Encerramento do IDTA antes do final do Prazo: as Partes não podem encerrar o IDTA antes do final do Prazo, a menos que haja uma violação do IDTA ou as Partes concordem por escrito. Encerrando o IDTA quando o IDTA Aprovado for alterado: Importador. O importador pode fazer mais transferências dos Dados Transferidos: Consulte o Schedule 1. Restrições específicas quando o Importador pode transferir os Dados Transferidos: Consulte o Schedule 1. Datas de Revisão: sempre que houver uma alteração nos Dados Transferidos, Finalidades, Informações do Importador, TRA ou avaliação de risco.

Tabela 3: Consulte o Schedule 1.

Tabela 4: Consulte a seção 3.3. Medidas Técnicas e Organizacionais para Garantir a Segurança dos Dados ("TOMs")

Schedule 3: Informações para SCC - Módulo 2

1. Sub-operadores

A VTEX utiliza Sub-operadores quando atua como Operador. O Cliente autoriza a VTEX a utilizar estes Sub-operadores de acordo com a Seção 5.3. Os sub-operadores estão disponíveis em nossa **Lista de sub-operadores**.

2. Períodos de retenção

A VTEX retém dados pessoais que coleta ou recebe do Cliente como Operador durante a vigência do Contrato e é consistente com suas obrigações neste DPA.

3. Informações para Transferências Internacionais

3.1. Para fins das Cláusulas Contratuais Padrão ou SCCs:

Cláusula 9, Módulo 2(a): As partes selecionam a Opção 2. O prazo é de 30 (trinta) dias.
Cláusula 11(a): As partes não selecionam a opção de resolução independente de disputas.
Cláusula 17, Módulo 2: As partes selecionam a Opção 2. O Estado-Membro do exportador de dados é o Estado-Membro da UE no qual o Cliente está localizado.
Cláusula 18 (b), Módulo 2: As Partes concordam que esses serão os tribunais do Estado Membro da UE nomeados no Contrato.

Anexo I(A): O exportador de dados é o Cliente. O importador dos dados é a Entidade VTEX indicada no Contrato. Os detalhes de contato do Cliente são os endereços de e-mail designados pelo Cliente na conta VTEX do Cliente. O contato da VTEX é dpo@vtex.com, ou conforme declarado no Contrato.

Anexo I (B): As partes concordam que **Schedule 1** descreve a transferência.

Anexo I (C): A autoridade de supervisão competente é a autoridade de supervisão nomeada pelo Cliente que atua como exportador de dados.

Anexo II: As partes concordam que o Schedule 3, Seção 3.3 descreve as medidas técnicas e organizacionais aplicáveis à transferência.

3.2. Para efeitos do Adendo do Reino Unido:

Tabela 1: O exportador de dados é Cliente. O importador dos dados é a Entidade VTEX indicada no Contrato. Os detalhes de contato do Cliente são os endereços de e-mail designados pelo Cliente na conta VTEX do Cliente. O contato da VTEX é dpo@vtex.com ou conforme previsto no Contrato.

Tabela 2: As Partes marcam a caixa de seleção que diz: “SCCs da UE aprovadas, incluindo as Informações do Apêndice e apenas com os seguintes módulos, cláusulas ou disposições opcionais das SCCs da UE aprovadas em vigor para os fins deste Adendo”, e a tabela anexa deverá ser considerado concluído de acordo com as preferências das Partes descritas no **Schedule 3, Seção 3.1 acima**.

Tabela 3: A Tabela 3 deverá ser preenchida com as informações previstas em (i) **Schedule 3, Seção 3.1 acima** em relação ao Anexo I(A), Anexo I(B), Anexo II e (ii) Anexo 3, Seção 1 acima em relação ao Anexo III.

Tabela 4: As Partes concordam que o importador de dados pode rescindir o Adendo do Reino Unido, conforme estabelecido na Seção 19 do Adendo do Reino Unido.

IDTA do Reino Unido será adicionado

Tabela 1: Consulte o Contrato.

Tabela 2: Lei do país do Reino Unido que rege o IDTA e local principal para reivindicações legais a serem feitas pelas Partes: Inglaterra e País de Gales. Status do Exportador e do Importador: Consulte o Schedule 1. Se o GDPR do Reino Unido se aplica ao Importador: Consulte o Contrato. Contrato e Prazo Vinculados: Consulte o Contrato. Encerramento do IDTA antes do final do Prazo: as Partes não podem encerrar o IDTA antes do final do Prazo, a menos que haja uma violação do IDTA ou as Partes concordem por escrito. Encerrando o IDTA quando o IDTA Aprovado for alterado: Importador. O importador pode fazer mais
transferências dos Dados Transferidos: Consulte o Schedule 1. Restrições específicas quando o Importador pode transferir os Dados Transferidos: Consulte o Schedule 1. Datas de Revisão: sempre que houver uma alteração nos Dados Transferidos, Finalidades, Informações do Importador, TRA ou avaliação de risco.

Tabela 3: Consulte o Schedule 1.

Tabela 4: Consulte a seção 3.3. Medidas Técnicas e Organizacionais para Garantir a Segurança dos Dados ("TOMs")

3.3. Medidas Técnicas e Organizacionais para Garantir a Segurança dos Dados ("TOMs")

O Importador de Dados implementou e manterá medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra uso indevido e perda ou destruição acidental conforme estabelecido nas Políticas de Privacidade e Segurança da VTEX.

As medidas técnicas e organizacionais atuais do Importador de Dados são definidas abaixo.

Conforme mencionado acima, 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 oferece ciclos de treinamento recorrentes, incluindo sessões gerais e específicas para funções, com forte ênfase em privacidade e segurança. A VTEX oferece treinamentos especializados em práticas seguras de desenvolvimento, alinhados às nossas certificações de segurança.

2. Proteção por senha
    a. As senhas são criptografadas usando PBKDF2 baseado em SHA-256. Durante este processo, apenas o valor hash resultante é armazenado, garantindo que as senhas originais permaneçam seguras e não sejam diretamente acessíveis.
    b. Os comerciantes podem optar por impor a expiração da senha após um período específico para usuários administradores.
    c. Os comerciantes também podem optar por integrar um provedor de identidade externo, permitindo-lhes definir suas próprias políticas de senha personalizadas.

3. Autorização e controle de acesso

A VTEX gerencia com eficiência os acessos lógicos, garantindo controle e monitoramento precisos das permissões de acesso aos sistemas e dados. Nossas práticas seguem políticas de segurança, incluindo medidas como o princípio do menor privilégio e segregação de funções. Os usuários têm acesso apenas ao estritamente necessário para suas funções, reduzindo o risco de exposição de informações confidenciais e reforçando a segurança de sistemas e dados.

4. Segurança de Endpoint
    a. A VTEX utiliza uma abordagem abrangente para mitigar ataques cibernéticos, empregando medidas como antivírus avançados, firewalls e filtros de conteúdo para bloquear malwares. Nossa plataforma inclui proteção contra ataques DDoS (Distributed Denial of Service) e outras ameaças.
    b. A VTEX também utiliza ferramentas de monitoramento para garantir segurança abrangente dos endpoints.

5. Classificação de dados
    a. A VTEX possui uma política de classificação de informações para determinar o nível adequado de proteção exigido para cada tipo de dado.

6. Registros de Logs

Todas as operações na plataforma são registradas automaticamente. Os erros da plataforma são registrados no software Security Information and Event Management, acessível à equipe VTEX para análise e melhoria do produto.

7. Gerenciamento de vulnerabilidades
    a. A VTEX realiza avaliações regulares de ameaças e vulnerabilidades em nossa plataforma e processos operacionais. Os riscos identificados levam a melhorias nos nossos sistemas de monitorização e notificação, permitindo-nos gerir potenciais problemas de forma eficaz, seja alertando o pessoal relevante ou iniciando ações automatizadas para mitigá-los ou eliminá-los. Para uma explicação detalhada dos nossos procedimentos de teste de penetração, consulte o ponto 14 do apêndice.

8. Certificações

a. De acordo com os padrões da indústria, as certificações das empresas geralmente cobrem o período de janeiro a dezembro, com dezembro marcando o início do processo de renovação para o próximo ano. Portanto, quando nos referimos às nossas certificações atuais, referimo-nos àquelas que foram mantidas durante o período aplicável mais recente. As certificações que a VTEX manteve durante esse período são as seguintes:"
    i. ISO 27001: Um padrão internacional para sistemas de gestão de segurança da informação.
    ii. SOC 1 - Tipo 2: Um relatório que abrange os controles internos dos sistemas de relatórios financeiros.
    iii. SOC 2 - Tipo 2: Um relatório que abrange Segurança, Disponibilidade, Integridade, Confidencialidade e Privacidade.
    iv. PCI: Uma validação de controles em torno dos dados do titular do cartão para reduzir fraudes com cartão de crédito.

Todas essas certificações podem ser solicitadas à VTEX a qualquer momento e estão disponíveis no link Seção de Compliance no VTEX Trust Hub (https://vtex.com/pt-br/trust/).

9. Como a VTEX aborda Backup e Redundância de Dados
    a. Os dados manipulados pela VTEX são armazenados em serviços AWS utilizando serviços gerenciados como S3, RDS e DynamoDB. Todos esses serviços fornecem infraestrutura de backup gerenciada pela AWS que é usada pela VTEX. A plataforma AWS é referência no setor de cloud computing e possui importantes certificações como: ISO 27001, PCI DSS, CSA, NIST e muitas outras. (Para ver uma lista de certificações detalhadas, acesse: https://aws.amazon.com/en/compliance/programs/).

10. Plano de Continuidade de Negócios e Plano de Recuperação de Desastres
    a. A VTEX possui um Plano de Recuperação de Desastres abrangente, que inclui políticas e procedimentos internos projetados para lidar com interrupções de serviço. Este plano visa restaurar os componentes afetados o mais rápido possível. Para garantir sua eficácia, a VTEX realiza testes regulares desse plano.
    b. O escopo deste plano é a Plataforma VTEX Cloud Commerce, incluindo: (i) todos os serviços que constituem a solução; (ii) todos os processos de negócio que o suportam ou ao seu funcionamento; (iii) todos os processos de negócio que suportam os clientes da VTEX que dependem da VTEX Cloud Commerce Platform;
    c. O Plano de Recuperação de Desastres da VTEX é suportado e implementado por processos automatizados que são acionados com base em ferramentas também automatizadas de monitoramento e notificação. Além disso, uma equipe especializada supervisiona esses processos e monitora seu desempenho para garantir a eficácia e a capacidade de resposta do plano.
    d. As partes interessadas externas 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 atual de integridade da plataforma VTEX True Cloud CommerceTM.

11. Criptografia de Dados Privados
    a. A VTEX garante a criptografia de acordo com o que exigem as regulamentações de privacidade e conformidade relacionadas à informações pessoais identificáveis. Os Módulos de Pagamentos são compatíveis com PCI e implementam criptografia de dados e rotação de chaves de acordo com os padrões PCI-DSS. A VTEX tem projetos de engenharia em andamento para implementar a criptografia e o isolamento de informações pessoais

identificáveis, bem como para implementar o registro de auditoria em uma infinidade de aplicações além daquelas que já o oferecem.

12. Armazenamento de Dados na VTEX
    a. O provedor de hospedagem da VTEX é a AWS, fornecedora líder mundial de serviços de computação em nuvem, e os dados são armazenados na região AWS da Virgínia do Norte, nos Estados Unidos.

13. Transmissão de Dados
    a. Todo o tráfego que entra na rede da VTEX é protegido pela tecnologia TLS 1.2 (ou superior) via http.

14. Políticas de Pentest
    a. Pela natureza do negócio da VTEX, estabelecemos uma política de realização de testes de penetração, ou *pentest*, pelo menos semestralmente. Adicionalmente, a nossa plataforma é regularmente avaliada por clientes, parceiros e auditores independentes, garantindo um escrutínio externo e interno contínuo.
    b. Os lojistas são incentivados a compartilhar os relatórios de pentest e notificações de vulnerabilidade com a VTEX, permitindo que nossa equipe de Segurança resolva prontamente quaisquer possíveis problemas identificados. Os testes de penetração devem ser previamente agendados com a VTEX. Qualquer teste realizado de forma autônoma sem aviso prévio à VTEX será considerado uma tentativa de ação não autorizada.

15. Avaliação de riscos de terceiros

A VTEX possui um processo abrangente de avaliação de nossos fornecedores para garantir que eles atendam aos nossos padrões de segurança e gestão de riscos. Utilizamos um questionário detalhado de avaliação de sub-operadores, que inclui perguntas relacionadas à segurança para avaliar riscos potenciais associados ao relacionamento de cada fornecedor. Os fornecedores considerados como apresentando riscos inaceitáveis são excluídos da adesão ao nosso ecossistema ou são contratualmente obrigados a implementar um plano de ação corretiva, se necessário. Por exemplo, a AWS, listada como Sub-operadora no Schedule 1, mantém certificações de segurança e privacidade ISO 27017:2015 e ISO 27018:2014, que são subconjuntos da ISO 27001:2013, o padrão de segurança mais rigoroso disponível.

16. Resposta a incidentes de segurança

A VTEX possui um protocolo formal de resposta a incidentes de segurança que abrange as etapas essenciais do processo: preparação, identificação do incidente, contenção, erradicação, recuperação e pós-incidente. Este procedimento inclui também um plano de comunicação integrado que é aplicado em todas as fases da resposta.

***