

ADENDO DE PROCESSAMENTO DE DADOS

Nota para cópia:

O Adendo de Processamento de Dados Privilegiados está disponível em <https://useinsider.com/legal/dpa/>.

Para os Clientes que desejarem receber uma cópia assinada do Adendo de Processamento de Dados do Insider, disponibilizamos essa cópia para você. Esta cópia inclui assinaturas na versão do Adendo de Processamento de Dados modificada pela última vez em 10 de junho de 2024. A Insider e suas afiliadas não aceitam quaisquer alterações a serem feitas nesta cópia, a menos que acordadas pelas Partes e feitas por escrito..

Observe que atualizamos o Contrato de Processamento de Dados conforme descrito no artigo "Alterações" abaixo. Os termos atuais do Contrato de Processamento de Dados estão disponíveis em "<https://useinsider.com/legal/dpa/>".

Se tiver alguma dúvida, entre em contato com o representante da Insider

Este Adendo de Processamento de Dados ("**DPA**") faz parte do Contrato Principal de Assinatura ou de outros contratos escritos ou eletrônicos entre a Insider e o Cliente (o "**Contrato**") para a compra de serviços on-line da Insider (identificados como "**Serviços**" ou de outra forma no contrato aplicável, e doravante definidos como "**Serviços**") para refletir o acordo das partes com relação ao Processamento de Dados Pessoais.

Ao assinar o Contrato, o Cliente celebra este DPA em seu próprio nome e, na medida exigida pelas Leis e Regulamentações de Proteção de Dados aplicáveis, em nome e por conta de seus Afiliados Autorizados, se e na medida em que a Insider processar Dados Pessoais para os quais esses Afiliados Autorizados se qualificam como Controlador. Apenas para os fins deste DPA, e exceto quando indicado de outra forma, o termo "Cliente" incluirá o Cliente e as Afiliadas Autorizadas. Todos os termos em maiúsculas não definidos neste documento terão o significado estabelecido no Contrato.

No decorrer da prestação dos Serviços ao Cliente nos termos do Contrato, a Insider poderá processar Dados Pessoais em nome do Cliente, e as Partes concordam em cumprir as seguintes disposições com relação a quaisquer Dados Pessoais, cada uma agindo razoavelmente e de boa fé. Para evitar dúvidas, cada referência ao DPA neste DPA significa este DPA, incluindo suas Programações.

TERMOS DE PROCESSAMENTO DE DADOS

1. DEFINIÇÕES

"**Afiliada autorizada**" significa qualquer Afiliada do Cliente que (i) esteja(i) está sujeita às leis e regulamentos de proteção de dados da União Europeia, do Espaço Econômico Europeu e/ou de seus estados membros e/ou do Reino Unido e/ou quaisquer outras leis e regulamentos de proteção de dados de outros países nos quais o Cliente ou sua Afiliada Autorizada estejam sediados ou prestem serviços, incluindo, entre outros, a República do Brasil (ii) tenha permissão para usar os Serviços de acordo com o Contrato entre o Cliente e a Insider, mas não tenha assinado seu próprio Formulário de Pedido com a Insider e não seja um "Cliente", conforme definido no Contrato.

"**Afiliada do Insider**" significa qualquer empresa na qual o Insider seja acionista e/ou tenha voz ativa em sua administração.

"**CCPA**" significa a Lei de Privacidade do Consumidor da Califórnia de 2018, Cal. Civ. Code § 1798.100 et seq., e suas regulamentações de implementação, conforme possam ser alteradas de tempos em tempos.

"**Controlador**" significa a entidade que determina as finalidades e os meios do Processamento de Dados Pessoais.

"**Dados do Cliente**" significa todos os dados ou informações eletrônicas enviados pelo Cliente ou em nome dele para, ou coletados do Aplicativo do Cliente pelos Serviços da Insider.

"**Leis e regulamentos de proteção de dados**" significa todas as leis e regulamentos, incluindo o GDPR, CCPA e LGPD aplicáveis a uma Parte em seu uso ou fornecimento dos Serviços, em conexão com o Processamento de Dados Pessoais nos termos do Contrato.

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

"**Documentação**" Refere-se a qualquer documento impresso ou digital, conteúdo da Insider Academy, apresentação, informação ou documento compartilhado em relação aos produtos e serviços da Insider e às atividades de processamento de dados da Insider.

"**GDPR**" significa o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

"**LGPD**" significa a Lei Geral de Proteção de Dados Brasileira, Lei 13.709/2018, que regula o tratamento de dados pessoais por

pessoas físicas e/ou jurídicas públicas e privadas, inclusive por meios eletrônicos, sobre a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

"Dados Pessoais" significa qualquer informação relacionada a uma pessoa física identificada ou identificável quando esses dados forem Dados do Cliente.

"Processamento" significa qualquer operação ou conjunto de operações realizadas sobre os Dados Pessoais, seja ou não por meios automáticos, tais como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização de outra forma, alinhamento ou combinação, restrição, exclusão ou destruição.

"Processador" significa a entidade que processa os dados pessoais em nome do Controlador.

"Violação de Dados Pessoais" significa uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a Dados Pessoais, transmitidos, armazenados ou processados pela Insider ou por seus subprocessadores, dos quais a Insider toma conhecimento.

"Folha de Dados de Segurança, Privacidade e Arquitetura" significa a Folha de Dados de Segurança, Privacidade e Arquitetura dos Serviços Insider, conforme atualizada periodicamente.

"Cláusulas Contratuais Padrão" ou **"SCC"** significa o acordo entre o Cliente e a Insider, de acordo com a decisão da Comissão Europeia sobre Cláusulas Contratuais Padrão para a transferência de dados pessoais para processadores estabelecidos em países terceiros que não garantem um nível adequado de proteção de dados, cuja cópia pode ser encontrada em <https://www.useinsider.com/legal>.

"Subprocessador" significa qualquer Processador contratado pela Insider ou seus Afiliados envolvidos no Processamento de Dados Pessoais.

2. PROCESSAMENTO DE DADOS PESSOAIS

2.1 Detalhes do Processamento. As partes reconhecem e concordam que, com relação ao Processamento de Dados Pessoais, o Cliente é o Controlador, a Insider é o Processador e que a Insider ou suas Afiliadas envolvidas no Processamento de Dados Pessoais contratarão Subprocessadores de acordo com os requisitos estabelecidos no Anexo 2 "Subprocessadores" abaixo. O objeto do Processamento de Dados Pessoais pela Insider é a execução dos Serviços nos termos do Contrato. A duração do Processamento, a natureza e a finalidade do Processamento, os tipos de Dados Pessoais e as categorias de Titulares de Dados Processados nos termos deste DPA estão especificados no Anexo 3 (Detalhes do Processamento) deste DPA.

2.2 Processamento de Dados Pessoais pelo Cliente. O Cliente deverá, em seu uso dos Serviços, Processar Dados Pessoais de acordo com as exigências das Leis e Regulamentações de Proteção de Dados. Para evitar dúvidas, as instruções do Cliente para o Processamento de Dados Pessoais deverão estar em conformidade com as Leis e Regulamentações de Proteção de Dados. O Cliente é responsável por todas as ações tomadas pelo Cliente ou por seus Usuários na(s) Conta(s) do Cliente e pela conformidade dos Usuários com este Contrato. O Cliente deverá fornecer aviso adequado e obter consentimento válido para o uso de tecnologias de rastreamento usadas pelos Serviços Insider na criação de perfis de Usuário Final que, se o Cliente estiver estabelecido no EEE ou se o Cliente usar os Serviços Insider em relação a residentes do EEE, deverá estar em conformidade com os arts. 13 e 7 do GDPR. Este DPA e o Contrato são, no momento da assinatura do Contrato, as instruções documentadas completas e finais do Cliente à Insider para o Processamento de Dados Pessoais, e a configuração dos Serviços pelo Cliente constituirá uma instrução adicional à Insider. Quaisquer instruções adicionais ou alternativas devem ser acordadas separadamente. O Cliente será o único responsável pela precisão, qualidade e legalidade dos Dados Pessoais e pelos meios pelos quais o Cliente adquiriu os Dados Pessoais.

2.3 Processamento de dados pessoais pela Insider. Insider shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of Customer and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Customer's Users in their use of the Services; (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., (iii) Processamento para cumprir outras instruções razoáveis documentadas fornecidas pelo Cliente (por exemplo, por e-mail), quando essas instruções forem consistentes com os termos do Contrato e (iv) Processamento quando vender serviços com base em determinado direito de propriedade intelectual; com base nas transferências de dados a serem feitas para fornecer o serviço ao proprietário principal do direito. A Insider processará os Dados Pessoais em conformidade com as Leis e Regulamentos de Proteção de Dados aplicáveis, desde que, no entanto, a Insider não viole essa obrigação contratual caso o Processamento de Dados Pessoais pela Insider em não conformidade com as Leis e Regulamentos de Proteção de Dados aplicáveis seja devido ao Cliente.

3. DIREITOS DOS TITULARES DE DADOS

3.1 Solicitações do Titular dos Dados. A Insider deverá, na medida do legalmente permitido e na medida em que puder identificar que a solicitação vem de um Titular de Dados cujos Dados Pessoais foram enviados aos Serviços pelo Cliente, notificar imediatamente o Cliente se a Insider receber uma solicitação de um Titular de Dados em relação ao exercício de qualquer Direito do Titular de Dados ("**Solicitação do Titular de Dados**"). A Insider confirmará ao Titular dos Dados que passou a solicitação ao Cliente, mas a Insider não tratará ou executará a Solicitação do Titular dos Dados.

3.2 Levando em conta a natureza do Processamento, a Insider deverá auxiliar o Cliente fornecendo medidas técnicas e organizacionais adequadas e necessárias, na medida do possível, para o cumprimento da obrigação do Cliente de responder a uma Solicitação do Titular dos Dados de acordo com as Leis e Regulamentações de Proteção de Dados.

4. PESSOAL INTERNO

4.1 Confidencialidade. A Insider deverá garantir que seu pessoal envolvido no Processamento de Dados Pessoais seja informado sobre a natureza confidencial dos Dados Pessoais, tenha recebido treinamento apropriado sobre suas responsabilidades e tenha assinado contratos de confidencialidade por escrito. A Insider deverá garantir que essas obrigações de confidencialidade sobrevivam ao término do contrato com o pessoal.

4.2 Confiabilidade. A Insider deverá tomar medidas comercialmente razoáveis para garantir a confiabilidade de qualquer funcionário da Insider envolvido no processamento de dados pessoais.

4.3 Limitação de Acesso. A Insider deverá garantir que o acesso da Insider aos Dados Pessoais seja limitado ao pessoal que estiver executando os Serviços de acordo com o Contrato.

4.4 Diretor de Proteção de Dados. A Insider nomeou um responsável pela proteção de dados para a Insider e suas Afiliadas. A pessoa nomeada pode ser contatada em privacy@useinsider.com.

5. SUB-PROCESSORES

5.1 Nomeação de Subprocessadores. O Cliente reconhece e concorda que (a) os Afiliados da Insider podem ser contratados como Subprocessadores; e (b) a Insider e os Afiliados da Insider, respectivamente, podem contratar Subprocessadores de terceiros em conexão com a prestação dos Serviços. A Insider ou um Afiliado da Insider celebrou um contrato por escrito com cada Subprocessador contendo obrigações de proteção de dados não menos protetoras do que as deste DPA com relação à proteção de Dados Pessoais na medida aplicável à natureza do produto e/ou serviços fornecidos por tal Subprocessador.

5.2 Lista de Subprocessadores Atuais e Notificação de Novos Subprocessadores. Anexada a este documento como Anexo 2 está uma lista atual de Subprocessadores para os Serviços. Essa lista de subprocessadores deve incluir as identidades desses subprocessadores, seu país de localização, bem como o tipo de processamento que eles realizam. A Insider notificará o Cliente sobre um novo Subprocessador(es) antes de autorizar qualquer novo Subprocessador(es) a Processar Dados Pessoais em conexão com o fornecimento dos Serviços aplicáveis.

5.3 Direito de objeção para novos subprocessadores. O Cliente pode se opor ao uso de um novo Subprocessador pela Insider, notificando-a prontamente por escrito dentro de dez (10) dias úteis após o recebimento da notificação da Insider, de acordo com o Anexo 2. Caso o Cliente se oponha a um novo Subprocessador, conforme permitido na frase anterior, a Insider envidará esforços razoáveis para disponibilizar ao Cliente uma alteração nos Serviços ou recomendará uma alteração comercialmente razoável na configuração ou no uso dos Serviços pelo Cliente para evitar o Processamento de Dados Pessoais pelo novo Subprocessador contestado, sem sobrecarregar o Cliente de forma injustificada. Se a Insider não puder disponibilizar essa alteração dentro de um período de tempo razoável, que não deverá exceder 30 (trinta) dias, o Cliente poderá rescindir o(s) Formulário(s) de Pedido aplicável(is) com relação apenas aos Serviços que não podem ser fornecidos pela Insider sem o uso do novo Subprocessador contestado, mediante notificação por escrito à Insider. A Insider reembolsará ao Cliente quaisquer taxas pré-pagas que cubram o restante do prazo do(s) Formulário(s) de Pedido após a data efetiva da rescisão com relação a esses Serviços rescindidos, sem impor uma penalidade ao Cliente por essa rescisão.

5.4 Responsabilidade pelos Subprocessadores. A Insider será responsável pelos atos e omissões de seus Subprocessadores na mesma medida em que a Insider seria responsável se estivesse executando os serviços de cada Subprocessador diretamente sob os termos deste DPA.

6. SEGURANÇA

6.1 Controles para a proteção dos dados do cliente. A Insider deverá manter medidas técnicas e organizacionais apropriadas para a proteção da segurança (incluindo a proteção contra a Violação de Dados Pessoais), confidencialidade e integridade dos Dados do Cliente, conforme estabelecido na Folha de Dados de Segurança, Privacidade e Arquitetura anexada ao presente como Anexo 1. A Insider monitora regularmente a conformidade com essas medidas. O Cliente é responsável por revisar as informações disponibilizadas pela Insider relacionadas à segurança de dados e por determinar de forma independente se os Serviços atendem aos requisitos e às obrigações legais do Cliente de acordo com as Leis e Regulamentos de Proteção de Dados. O Cliente reconhece que as medidas de segurança descritas na Folha de Dados de Segurança, Privacidade e Arquitetura estão sujeitas a progresso e desenvolvimento técnico e que a Insider pode atualizar ou modificar esse documento periodicamente, desde que essas atualizações e modificações não resultem em uma diminuição significativa da segurança geral dos Serviços durante o período de assinatura.

6.2 Gerenciamento e Notificação de Incidentes de Dados do Cliente. A Insider mantém políticas e procedimentos de gerenciamento de incidentes de segurança especificados na Folha de Dados de Segurança, Privacidade e Arquitetura e deverá notificar o Cliente sem atrasos indevidos após tomar conhecimento de uma Violação de Dados Pessoais. A Insider fornecerá as informações ao Cliente necessárias para permitir que o Cliente cumpra suas obrigações sob as Leis e Regulamentos de Proteção de Dados em relação a tal Violação de Dados Pessoais. O conteúdo dessa comunicação ao Cliente (i) incluirá a natureza do Processamento e as informações disponíveis para a Insider, e (ii) levará em conta que, de acordo com as Leis e Regulamentações de Proteção de Dados aplicáveis, o Cliente poderá precisar notificar os reguladores ou indivíduos sobre o seguinte: (a) uma descrição da natureza da Violação de Dados Pessoais, incluindo, quando possível, as categorias e o número aproximado de indivíduos em questão e as categorias e o número aproximado de registros de Dados Pessoais em questão; (b) uma descrição das prováveis consequências da Violação de Dados Pessoais; e (c) uma descrição das medidas tomadas ou propostas para serem tomadas para lidar com a Violação de Dados Pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos. A Insider envidará esforços comercialmente razoáveis para identificar a causa de tal Violação de Dados Pessoais e tomará as medidas que considerar necessárias e razoáveis para remediar a causa de tal Violação de Dados Pessoais, na medida em que a remediação esteja dentro do controle razoável da Insider. A obrigação de remediar a causa de uma Violação de Dados Pessoais não se aplicará a Violações de Dados Pessoais causadas pelo Cliente ou pelos Usuários do Cliente.

6.3 Certificações e auditorias de terceiros. A Insider obteve as certificações e auditorias de terceiros estabelecidas na Folha de Dados de Segurança, Privacidade e Arquitetura. Mediante solicitação por escrito do Cliente, em intervalos razoáveis, e sujeita às obrigações de confidencialidade estabelecidas no Contrato, a Insider disponibilizará ao Cliente (ou ao auditor terceirizado independente do Cliente que não seja concorrente da Insider e que esteja sujeito a obrigações de confidencialidade substancialmente semelhantes àquelas estabelecidas no Contrato) uma cópia das auditorias ou certificações de terceiros mais recentes da Insider, conforme aplicável, que a Insider disponibiliza aos seus clientes em geral.

7. DEVOLUÇÃO E EXCLUSÃO DE DADOS DO CLIENTE

A Insider devolverá os Dados do Cliente, permitindo que o Cliente exporte seus Dados do Cliente, conforme estabelecido no Contrato, e excluirá os Dados do Cliente, de acordo com este DPA, o Contrato, as leis aplicáveis e a Documentação.

8. AFILIADAS

8.1 Relacionamento entre a Insider e as Afiliadas Autorizadas do Cliente. As partes reconhecem e concordam que, ao assinar o Contrato, o Cliente celebra este DPA em seu próprio nome e, conforme aplicável, em nome e por conta de seus Afiliados Autorizados, estabelecendo assim um DPA independente entre a Insider e cada um desses Afiliados Autorizados, sujeito às disposições do Contrato e desta Seção 8 e Seção 9. Cada Afiliado Autorizado concorda em estar vinculado às obrigações previstas neste DPA e, na medida do aplicável, no Contrato. Para fins de clareza, uma Afiliada Autorizada não é e não se torna parte do Contrato e é apenas parte deste DPA. Todo acesso e uso dos Serviços por Afiliados Autorizados devem estar em conformidade com os termos e condições do Contrato e qualquer violação dos termos e condições do Contrato por um Afiliado Autorizado será considerada uma violação pelo Cliente.

8.2 Comunicação. O Cliente que é a parte contratante do Contrato permanecerá responsável por coordenar toda a comunicação com a Insider nos termos deste DPA e terá o direito de fazer e receber qualquer comunicação em relação a este DPA em nome de suas Afiliadas e Afiliadas Autorizadas.

8.3 Direitos de Controlador de Dados de Afiliadas e Afiliadas Autorizadas. Qualquer Afiliada ou Afiliada Autorizada deverá, na medida em que e somente se exigido pelas Leis e Regulamentações de Proteção de Dados aplicáveis, ter o direito de exercer os

direitos e buscar recursos sob este DPA, sujeito ao seguinte:

Exceto quando as Leis e Regulamentações de Proteção de Dados aplicáveis exigirem que a Afiliada ou a Afiliada Autorizada exerça um direito ou busque qualquer recurso nos termos deste DPA contra a Insider diretamente por si mesma, as partes concordam que:

(i) somente o Cliente que é a parte contratante do Contrato deverá exercer tal direito (incluindo qualquer direito de Auditoria) ou buscar qualquer recurso em nome de tal Afiliado ou Afiliado Autorizado,

(ii) o Cliente, que é a parte contratante do Contrato, deverá exercer tais direitos nos termos deste DPA não separadamente para cada Afiliada ou Afiliada Autorizada individualmente, mas de forma combinada para todas as suas Afiliadas e Afiliadas Autorizadas em conjunto, e

(iii) ao realizar uma Auditoria no local, tomar todas as medidas razoáveis para limitar qualquer impacto sobre o Insider e seus Subprocessadores, combinando, na medida do razoavelmente possível, várias solicitações de Auditoria realizadas em nome de diferentes Afiliados e Afiliados Autorizados em uma única Auditoria.

Para os fins desta Seção 8.3, um Afiliado que assina um Formulário de Pedido com a Insider não é considerado "Cliente".

9. LIMITAÇÃO DE RESPONSABILIDADE

A responsabilidade de cada uma das partes e de todas as suas Afiliadas, consideradas em conjunto, decorrentes ou relacionadas a este DPA e a todos os DPAs entre as Afiliadas Autorizadas, a Insider e as Afiliadas da Insider, seja em contrato, ato ilícito ou sob qualquer outra teoria de responsabilidade, está sujeita à seção "Limitação de Responsabilidade" do Contrato, e qualquer referência nessa seção à responsabilidade de uma parte significa a responsabilidade agregada dessa parte e de todas as suas Afiliadas nos termos do Contrato e de todos os DPAs em conjunto.

10. DISPOSIÇÕES ESPECÍFICAS DA EUROPA

10.1 Avaliação do impacto da proteção de dados. Mediante solicitação do Cliente, a Insider fornecerá ao Cliente a cooperação e a assistência razoáveis necessárias para cumprir a obrigação do Cliente, nos termos do GDPR, de realizar uma avaliação do impacto da proteção de dados relacionada ao uso dos Serviços pelo Cliente, na medida em que o Cliente não tenha acesso às informações relevantes e na medida em que tais informações estejam disponíveis para a Insider. A Insider deverá fornecer assistência razoável ao Cliente na cooperação ou consulta prévia com a Autoridade Supervisora (conforme definido no GDPR) no desempenho de suas tarefas relacionadas a esta Seção 10.1 deste DPA, na medida exigida pelo GDPR.

10.2 Instruções infratoras. A Insider deverá informar imediatamente o Cliente se, em sua opinião, uma instrução infringir o GDPR.

10.3 Direito de auditoria europeia. Quando o Cliente, uma Afiliada ou uma Afiliada Autorizada estiver sujeito às leis de privacidade da União Europeia, da Suíça, do Espaço Econômico Europeu e/ou de seus estados membros e do Reino Unido, a Insider deverá permitir e contribuir para auditorias e inspeções ("Auditorias") conduzidas pelo Cliente (ou pelo auditor independente do Cliente), independente e terceirizado do Cliente que não seja concorrente da Insider e que esteja sujeito a obrigações de confidencialidade substancialmente semelhantes às aquelas estabelecidas no Contrato), fornecendo quaisquer informações relativas à conformidade da Insider com as obrigações estabelecidas neste DPA na forma de uma cópia das auditorias ou certificações terceirizadas mais recentes da Insider, conforme aplicável, que a Insider disponibiliza aos seus clientes em geral. Quando o Cliente desejar realizar uma Auditoria no local, ele poderá fazê-lo até uma (1) vez por ano, com aviso prévio por escrito de pelo menos três (3) semanas, a menos que seja exigido de outra forma pelos reguladores do Cliente, de sua Afiliada ou de sua Afiliada Autorizada ou pela lei aplicável a qualquer um deles. Se o Cliente solicitar uma Auditoria no local, os seguintes termos se aplicarão: (a) essa Auditoria deverá ser limitada às instalações operadas pela Insider, (b) essa Auditoria não deverá exceder um (1) dia útil; (c) antes do início de qualquer Auditoria, o Cliente e a Insider deverão concordar mutuamente sobre o escopo, o custo e o cronograma da Auditoria; e (d) o Cliente deverá notificar imediatamente a Insider com informações sobre qualquer não conformidade descoberta durante o curso de uma Auditoria.

10.4 Mecanismo(s) de transferência para transferências de dados. A partir da Data de Entrada em Vigor deste DPA, com relação a quaisquer transferências de Dados Pessoais nos termos deste DPA da União Europeia, da Suíça, do Espaço Econômico Europeu e/ou de seus estados-membros e do Reino Unido para países que não garantem um nível adequado de proteção de dados dentro do significado das Leis e Regulamentações de Proteção de Dados dos territórios acima mencionados, na medida em que tais transferências estejam sujeitas a tais Leis e Regulamentações de Proteção de Dados, a Insider disponibiliza o(s) seguinte(s) mecanismo(s) de transferência que deverá(ão) ser aplicado(s), na ordem de precedência conforme estabelecido abaixo, se aplicável:

i. Qualquer mecanismo de transferência válido, de acordo com o Capítulo V "Transferências de dados pessoais para países terceiros ou organizações internacionais" do GDPR, que permita a transferência de Dados Pessoais da UE para fora da UE, que a Insider assinaria,

certificaria ou participaria.

ii. As Cláusulas Contratuais Padrão, de acordo com os seguintes termos:

1. Para os fins das SCC, quando e conforme aplicável, o Cliente e quaisquer Afiliadas Autorizadas aplicáveis são, cada um, o exportador de dados, e a assinatura do Cliente deste DPA ou de um Contrato que faça referência a este DPA, ou a assinatura de um Formulário de Pedido por uma Afiliada do Cliente nos termos de um Contrato que faça referência a este DPA, será tratada como assinatura das SCC e de seus anexos. A assinatura do Insider deste DPA ou de um Contrato que faça referência a este DPA será tratada como assinatura da SCC e de seus anexos. No caso de qualquer conflito ou inconsistência entre este DPA e a SCC, a SCC deverá prevalecer.

2. O Anexo 2 deste DPA representa o consentimento expresso do Cliente com relação aos Subprocessadores novos e existentes.

11. ALTERAÇÕES

Não obstante qualquer outra disposição em contrário no Contrato, reservamo-nos o direito de fazer quaisquer atualizações e alterações neste DPA, e os termos aplicáveis na seção "Alteração; Sem Renúncia" dos Termos Principais serão aplicados.

12. SEVERABILIDADE

Se qualquer disposição individual deste DPA for considerada inválida ou inexecutável, a validade e a exequibilidade das outras disposições deste DPA não serão afetadas.

13. Lei de Direitos de Privacidade da Califórnia de 2020

13.1. O seguinte se aplica aos Clientes sujeitos à CPRA:

a) Todas as referências às Leis e Regulamentações de Proteção de Dados neste ATD devem ser consideradas como incluindo uma referência à CPRA;

b) Todas as referências a Dados Pessoais neste DPA devem ser consideradas como incluindo Informações Pessoais, conforme definido na CPRA, desde que tais dados sejam Dados do Cliente;

c) Todas as referências a "Controlador" neste DPA devem ser consideradas referências a "Empresa", conforme definido na CPRA;

d) Todas as referências a "Processador" neste DPA serão consideradas referências a "Provedor de Serviços", conforme definido na CPRA;

e) Qualquer termo em letra maiúscula usado nesta Seção 11, mas não definido neste documento, terá o significado estabelecido nos CPRA.

13.2. A Insider não venderá nenhuma Informação Pessoal.

13.3. A Insider processará as Informações Pessoais somente conforme estabelecido na Seção 2.3 (a "Finalidade Comercial") e não reterá, usará ou divulgará as Informações Pessoais para qualquer outra finalidade que não seja a Finalidade Comercial.

13.4. A Insider não recebe quaisquer Informações Pessoais do Cliente como contrapartida pela prestação dos Serviços pela Insider.

13.5. A Insider certifica que entende as restrições estabelecidas nesta Seção 11 e que as cumprirá.

14. DISPOSIÇÕES ESPECÍFICAS DA LEGISLAÇÃO BRASILEIRA

As disposições estabelecidas nesta Seção 14 aplicam-se a todo e qualquer Afiliado Autorizado, Afiliado Insider e Parceiros sujeitos à LGPD e a outras leis e regulamentos brasileiros relacionados à proteção de dados.

14.1. **Avaliação de Impacto na Proteção de Dados.** Na medida em que o Cliente é obrigado a fornecer a Avaliação de Impacto na Proteção de Dados perante a Autoridade Nacional de Proteção de Dados ("ANPD") e nos termos previstos na Lei Geral de Proteção de Dados ("Lei n. 13.709/2018" ou "LGPD"), mediante solicitação do Cliente, a Insider fornecerá ao Cliente a cooperação e a assistência razoáveis necessárias para cumprir a obrigação do Cliente, nos termos da LGPD, de realizar uma avaliação do impacto da proteção de dados relacionada ao uso dos Serviços pelo Cliente, na medida em que o Cliente não tenha acesso às informações relevantes e na medida em que tais informações estejam disponíveis para a Insider. A Insider deverá fornecer assistência razoável ao Cliente na cooperação ou consulta prévia com a Autoridade Supervisora (conforme definido na LGPD) no desempenho de suas tarefas relacionadas a esta Seção 14.1 deste DPA, na medida exigida pela LGPD.

14.2. **Mecanismos para Transferência Internacional de Dados Pessoais.** Na medida em que a Insider for obrigada a proceder com a transferência internacional de Dados Pessoais para a execução dos Serviços nos termos do Contrato e deste DPA, a Insider deverá cumprir as disposições das Leis e Regulamentos de Proteção de Dados, particularmente com a LGPD e qualquer outra regulamentação

emitida pela ANPD sobre esse assunto. Sempre que a Insider transferir Dados Pessoais para países terceiros, a Insider deverá garantir a confidencialidade, disponibilidade e integridade dos Dados Pessoais, aplicando todas as questões de segurança técnica e organizacional previstas neste DPA, bem como cumprir com a transferência internacional de Dados Pessoais com base legal prevista no Artigo 33 da LGPD e outras obrigações decorrentes de quaisquer regulamentos emitidos pela ANPD, conforme aplicável.

14.3. Responsabilidade sobre o processamento de dados de acordo com as leis brasileiras de proteção de dados. Sem prejuízo dos termos previstos na Seção 9 deste DPA, as Partes reconhecem e concordam que o Cliente, como Controlador de Dados, é o responsável direto perante terceiros por quaisquer perdas e danos decorrentes do processamento de Dados Pessoais nos termos do Contrato e deste DPA. Nesse sentido, o Cliente defenderá, indenizará e isentará a Insider de e contra toda e qualquer reivindicação, demanda, ação ou processo de terceiros (a) decorrentes ou relacionados ao uso dos Serviços da Insider pelo Cliente em violação de quaisquer Leis e Regulamentos de Proteção de Dados, conforme aplicável, ou ao Contrato ou a este DPA, (b) decorrentes de quaisquer instruções fornecidas pelo Cliente à Insider para o processamento de Dados Pessoais nos termos do Contrato e deste DPA, e indenizará a Insider de e contra quaisquer perdas, danos, responsabilidades, penalidades, danos punitivos, despesas, honorários advocatícios razoáveis e custos de qualquer tipo ou valor que surjam, exceto na medida em que tais reivindicações, perdas, danos ou responsabilidades sejam diretamente atribuíveis à não conformidade ou falha da Insider relacionada ao processamento de Dados Pessoais em seus Serviços.

Lista de programações:

Cronograma 1: Folha de dados de segurança interna, privacidade e arquitetura

Anexo 2: Lista de subprocessadores a partir da data de vigência

Anexo 3: Detalhes do processamento

ESQUEMA 1

Segurança interna, privacidade e arquitetura Folha de dados de segurança da informação

Introdução

O objetivo deste documento é fornecer informações de alto nível aos nossos clientes sobre o compromisso da Insider com a segurança e a proteção de dados.

Compromisso de confiança corporativa do insider

A Insider tem o compromisso de conquistar e manter a confiança de nossos clientes. Nosso objetivo é ser o mais transparente possível com nossos clientes, oferecendo segurança e proteções de última geração para atender e superar as expectativas no mundo da computação moderna de hoje.

Propriedade da política

A Insider tem uma política de segurança de informações documentada que todos os funcionários devem ler e reconhecer. Essa política é revisada e atualizada anualmente. O desenvolvimento, a manutenção e a emissão da política de segurança são de responsabilidade da Equipe de Segurança da Insider.

Infraestrutura privilegiada

A Insider hospeda os Serviços Insider com a Amazon Web Services em sua região EU-West-1, na Irlanda.

Arquitetura de terceiros

A Insider pode usar uma ou mais redes de entrega de conteúdo de terceiros para fornecer os Serviços Insider e otimizar a entrega de conteúdo através dos Serviços Insider. Os itens de conteúdo a serem fornecidos aos assinantes ou usuários finais, como imagens ou anexos carregados nos Serviços Insider, podem ser armazenados em cache nessas redes de fornecimento de conteúdo para agilizar a transmissão. As informações transmitidas por uma rede de fornecimento de conteúdo podem ser acessadas por essa rede de fornecimento de conteúdo exclusivamente para permitir essas funções.

Auditorias, certificações e conformidade normativa

A Insider é certificada pela ISO/IEC 27001 e tem o relatório SOC 2 Tipo 1 apenas para seus próprios produtos. A Insider também celebra as Cláusulas Contratuais Padrão da UE com seus clientes que gostariam de ser protegidos com mecanismos de transferência de dados aplicáveis de acordo com o GDPR.

Controles de segurança

1. Segurança da organização

O CTO da Insider é responsável pela segurança geral dos Serviços Insider, incluindo os produtos Mind Behind, incluindo supervisão e

responsabilidade. Os contratos da Insider com provedores de hospedagem terceirizados, como a Amazon Web Services, incluem requisitos de proteção de informações padrão do setor.

2. Classificação de ativos e controle de acesso lógico

A Insider mantém um inventário de ativos de informações essenciais, como servidores, bancos de dados e informações. Todos os Dados do Cliente são classificados como Confidenciais pela Insider.

A Insider adota o princípio do menor privilégio para todas as contas que executam serviços de aplicativos ou bancos de dados, bem como para sua própria equipe. A Insider mantém ambientes separados de desenvolvimento, preparação (ou sandbox), teste de aceitação do usuário e produção; o acesso a cada ambiente e dentro de cada ambiente é estritamente controlado.

O acesso aos servidores da Insider é controlado por meio de chaves SSH revogáveis gerenciadas pelo gerenciamento de configuração e rotacionadas pelo menos anualmente. Todo o acesso aos servidores da Insider ou aos Dados do Cliente é registrado e só pode ser acessado por meio da VPN da Insider, que usa autenticação multifator. O acesso ao banco de dados é controlado por senhas de 24 caracteres com lista de permissões de IP. Os processos de onboarding e off-boarding de RH da Insider lidam com o provisionamento e o desprovisionamento de contas e acessos.

3. Segurança do pessoal

Todos os funcionários da Insider assinam um acordo de não divulgação quando começam a trabalhar. Além disso, a Insider realiza verificações de antecedentes de seus funcionários como parte de seu processo de integração. Todos os funcionários são informados e concordam em cumprir as políticas e práticas de segurança da Insider como parte de sua integração inicial.

Os administradores de sistemas, desenvolvedores e outros usuários com acesso privilegiado recebem treinamento especial e contínuo e são submetidos a uma triagem adicional de antecedentes.

4. Segurança física e ambiental

O acesso às instalações da Insider é controlado por segurança 24 horas por dia. Além disso, todos os escritórios da Insider são protegidos por acesso trancado e estão sob vigilância por vídeo 24 horas por dia. Todas as estações de trabalho dos funcionários da Insider são criptografadas e protegidas por senha, e todas as contas de usuário da Insider exigem autenticação de dois fatores.

Os data centers e servidores são gerenciados e controlados por nossos provedores de hospedagem na nuvem. Os funcionários da Insider não têm acesso a nenhum desses centros de dados.

Detalhes sobre as práticas e os controles de segurança aplicáveis a essas instalações podem ser encontrados em seus sites: AWS: <https://aws.amazon.com/security>

5. Políticas e registro em log

Os Serviços Insider e seus próprios produtos são operados de acordo com os seguintes procedimentos para aumentar a segurança:

As senhas de usuário nunca são transmitidas ou armazenadas em texto claro

O insider usa métodos padrão do setor para determinar a validade da senha

O Insider mantém registros de auditoria para todos os acessos aos servidores de produção

O acesso ao servidor é controlado pelo Amazon Web Services Identity and Access Management

Os registros são armazenados em um host centralizado e seguro para evitar adulterações

As senhas não são registradas em nenhuma circunstância

Todo o acesso às contas do painel do cliente por funcionários internos deve ser feito por meio de um serviço interno que seja acessível somente por meio de uma VPN de dois fatores.

Como parte da Política de Segurança de Informações dos Funcionários da Insider, os funcionários não podem armazenar quaisquer Dados do Cliente em mídia removível

6. Detecção de intrusão

A Insider monitora o comportamento de sistemas, usuários e arquivos em toda a sua infraestrutura usando um Sistema de Detecção de Intrusão baseado em host. Os alertas de Detecção de Intrusão são monitorados pelas equipes de Segurança e DevOps 24 horas por dia, 7 dias por semana. Além disso, a Insider pode analisar os dados coletados pelos navegadores da Web dos usuários (por exemplo, tipo de dispositivo, resolução de tela, fuso horário, versão do sistema operacional, tipo e versão do navegador, fontes do sistema, plug-ins de navegador instalados, tipos de MIME ativados, etc.) para fins de segurança, inclusive para detectar navegadores comprometidos, para evitar autenticações fraudulentas e para garantir que os Serviços Insider funcionem adequadamente.

As APIs e o Dashboard da Insider usam controles de acesso rigorosos baseados em funções e permissões de usuário. Solicitações da Web e chamadas de API não autorizadas são registradas e alertam automaticamente a equipe de engenharia do Insider.

7. Registros de segurança

Todos os sistemas da Insider usados no fornecimento dos Serviços Insider, incluindo firewalls, roteadores, switches de rede e sistemas operacionais, registram informações em seus respectivos recursos de registro do sistema para permitir revisões e análises de segurança.

8. Patching do sistema e gerenciamento de configuração

A Insider aplica patches em seus servidores e reconstrói toda a sua infraestrutura de nuvem a partir de sistemas de gerenciamento de configuração regularmente, o que garante que os patches mais recentes sejam aplicados e que nós "reiniciemos" de volta a um estado conhecido e limpo. A Insider mantém vários ambientes e testa as alterações em ambientes de desenvolvimento em contêineres e em ambientes de preparação ao vivo antes de fazer alterações nos ambientes de produção.

9. Gerenciamento de vulnerabilidades

A infraestrutura e os aplicativos da Insider são continuamente examinados por um sistema de gerenciamento de vulnerabilidades. Os alertas são monitorados pela nossa equipe de segurança e tratados pelo menos mensalmente pela equipe de segurança da Insider. A Insider também é membro de várias listas de discussão sobre vulnerabilidades CVE. Os patches e as vulnerabilidades "críticas" e "altas" são corrigidos no prazo máximo de 30 dias após a descoberta.

O Insider também usa ferramentas de análise de código estático durante o processo de compilação (como Brakeman e bundler-audit) para realizar a análise de segurança estática.

10. Teste de penetração de terceiros

A Insider passa por um teste de penetração de terceiros dos Serviços Insider anualmente.

11. Monitoramento

Para os processos de monitoramento técnico, manutenção e suporte, a Insider usa uma combinação de ferramentas para garantir que os processos e servidores estejam funcionando corretamente, incluindo, entre outros, os seguintes:

Monitoramento de processos

Monitoramento de CPU, disco e memória

Monitoramento do tempo de atividade

Monitoramento funcional

Monitoramento do banco de dados

Monitoramento do desempenho do APM

Monitoramento da latência

Monitoramento de erros

12. Controle de acesso do cliente

Os Insider Services empregam uma variedade de controles de segurança. Esses controles incluem, mas não estão limitados a:

Lista de permissões de IP da API - Define o intervalo de endereços IP a partir dos quais os usuários de um cliente podem acessar a API do Insider para evitar que terceiros não autorizados acessem os serviços do Insider.

Todas as solicitações no Insider Dashboard têm proteção contra falsificação de solicitações entre sites (CSRF). Todos os serviços da Web usam HTTPS criptografado para todo o tráfego e não permitem todo o tráfego HTTP via HTTP Strict Transport Security ("HSTS").

Tentativas de login fracassadas são registradas e uma conta é bloqueada com o proprietário notificado após várias tentativas fracassadas.

13. Desenvolvimento e manutenção

O Insider usa ferramentas como o GitHub para gerenciar com eficácia o ciclo de vida do desenvolvimento. Durante os testes, o Insider gera contas de teste e dados falsos para testes. O Insider não usa dados de produção em contas de teste.

O controle de origem do aplicativo é realizado por meio de repositórios privados do GitHub. A Insider possui controles para garantir que todo o código seja aprovado antes de ser mesclado ao ramo de código principal da Insider; somente funcionários autorizados têm acesso para promover o código para produção.

Os desenvolvedores da Insider recebem treinamento de segurança adicional como parte de sua integração e passam por treinamentos de segurança regulares e periódicos durante o período de seu emprego. A Insider mantém uma lista de princípios básicos de segurança para engenharia e diretrizes de alto nível sobre tópicos de segurança para o desenvolvimento seguro de software.

14. Prevenção de malware

O Insider adota o princípio do privilégio mínimo para todas as contas que executam aplicativos ou serviços de banco de dados. O gerenciamento adequado de alterações garante que somente os pacotes autorizados sejam instalados por meio de um sistema de

gerenciamento de pacotes que contenha somente software confiável e que o software nunca seja instalado manualmente. Todos os computadores dos funcionários da Insider têm scanners de vírus instalados e definições atualizadas enviadas por uma plataforma central de gerenciamento de dispositivos.

15. Gerenciamento de incidentes de segurança da informação

O Insider mantém políticas e procedimentos de gerenciamento de incidentes de segurança por escrito e regularmente auditados, incluindo um Plano de Resposta a Incidentes a ser implementado no caso de um incidente.

16. Criptografia de dados

Os Insider Services usam práticas de criptografia aceitas pelo setor para proteger os Dados do Cliente e as comunicações durante as transmissões entre a rede do cliente e os Insider Services, incluindo Certificados TLS de 256 bits e chaves públicas RSA de 4096 bits, no mínimo.

A Insider audita as cifras TLS usadas em conexão com o fornecimento dos Serviços com auditores de segurança terceirizados para garantir que não sejam usadas cifras anônimas ou fracas. Essas auditorias também confirmam que os Serviços não permitem a renegociação do cliente, suportam proteção contra ataques de downgrade e sigilo de encaminhamento.

Os dados enviados para a Amazon Web Services são criptografados em trânsito e em repouso usando a criptografia AES-256 por meio do processo de chave de criptografia gerenciada da Amazon.

Quando o uso dos Serviços exige que o cliente forneça acesso a serviços de terceiros, a Insider realiza a criptografia adicional dessas informações.

17. Devolução e exclusão de dados do cliente

Os Serviços Insider permitem a importação, exportação e exclusão de Dados do Cliente por usuários autorizados em todos os momentos durante a vigência da assinatura de um cliente. Após a rescisão ou expiração dos Serviços, a Insider deverá sobrescrever ou excluir com segurança os Dados do Cliente no prazo de 180 dias após tal rescisão, de acordo com o Contrato, as leis aplicáveis e a Documentação.

18. Confiabilidade e backup

Todos os componentes de rede, aceleradores de SSL, balanceadores de carga, servidores da Web e servidores de aplicativos são configurados de forma redundante. Todos os dados do cliente enviados aos Insider Services são armazenados em um servidor de banco de dados múltiplo com vários clusters ativos para maior disponibilidade. Todos os servidores de banco de dados são replicados quase em tempo real e o backup é feito regularmente. Os backups são criptografados usando a criptografia AES-256 e verificados quanto à integridade.

19. Gerenciamento da continuidade dos negócios e recuperação de desastres

A Insider tem um Procedimento de Continuidade de Negócios e um Plano de Recuperação de Desastres formais e documentados, que são testados anualmente. A Insider testa backups de banco de dados e failovers como parte do nosso Plano de Continuidade de Negócios.

20. Bloqueio de acesso de terceiros

Os Serviços Insider não foram projetados para incluir backdoors ou funcionalidades semelhantes que permitam que o governo ou terceiros acessem os Dados do Cliente. Não fornecemos voluntariamente a nenhum governo ou terceiro chaves de criptografia ou qualquer outra forma de quebrar nossa criptografia.

21. Contatos

A Equipe de Segurança da Insider pode ser contatada pelo e-mail security@useinsider.com.

REGRA 2

SUBPROCESSADORES USADOS EM CONEXÃO COM OS SERVIÇOS INTERNOS

A lista de subprocessadores do Insider está disponível em <https://useinsider.com/legal/subprocessors>

REGRA 3

DETALHES DO PROCESSAMENTO

Natureza e finalidade do processamento

A Insider processará os Dados Pessoais conforme necessário para executar os Serviços de acordo com o Contrato, conforme

especificado na Documentação e conforme instruído pelo Cliente em seu uso dos Serviços.

Duração do processamento

Sujeito à Seção 7 da DPA, a Insider processará os Dados Pessoais durante a vigência do Contrato, a menos que acordado de outra forma por escrito.

Categorias de titulares de dados

O Cliente poderá enviar Dados Pessoais aos Serviços, cuja extensão é determinada e controlada pelo Cliente a seu exclusivo critério, e que incluem Dados Pessoais relacionados aos Usuários Finais (clientes do Cliente).

Tipo de dados pessoais

Informações de transação (informações de pedido/solicitação do usuário final do Cliente)

Informações de marketing (informações obtidas por meio do Insider Java Script, que é uma tecnologia semelhante a um cookie)

Informações sobre cliques

Comportamento de navegação (páginas visitadas no site, produtos ou serviços visualizados, tempo gasto em cada página, frequência de visitas)

Duração da permanência no site/anúncio

Endereço IP

Respostas a pesquisas

Histórico de compras (itens comprados, histórico de transações, valor do pedido)

Informações do dispositivo (tipo de dispositivo (desktop, celular, tablet), sistema operacional, tipo e versão do navegador)

Embora não esteja incluído no curso normal dos Serviços Insider, se o Cliente preferir enviar os seguintes dados para usar recursos específicos dos Serviços Insider, a Insider processará as seguintes categorias de Dados Pessoais:

Informações de contato (e-mail, número de telefone)

Informações de identidade (nome, sobrenome, idade, sexo, data de nascimento dos usuários do site, localização, IDFA)

ACEITO PELO CLIENTE

ACEITO PELO INSIDER

SIGNATURE: _____

SIGNATURE: _____

FULL NAME: _____

FULL NAME: _____

TITLE: _____

TITLE: _____

DATE: _____

DATE: _____

Anexo 1: CLÁUSULAS CONTRATUAIS PADRÃO

O objetivo dessas cláusulas contratuais padrão é fornecer garantias adequadas na aceção do artigo 46(1) e (2)(c) do Regulamento (UE) 2016/679 para a transferência por um controlador ou processador de dados pessoais processados sujeitos a esse regulamento (exportador de dados) para um controlador ou (sub)processador cujo processamento dos dados não esteja sujeito a esse regulamento (importador de dados). As cláusulas contratuais padrão também estabelecem os direitos e obrigações dos controladores e processadores com relação aos assuntos mencionados no artigo 28 (3) e (4) do Regulamento (UE) 2016/679, no que diz respeito à transferência de dados pessoais de um controlador para um processador ou de um processador para um subprocessador.

Cada uma das "**Partes**"; em conjunto, as "**Partes**", concordaram com as seguintes Cláusulas Contratuais ("**Cláusulas**") a fim de introduzir salvaguardas adequadas com relação à proteção da privacidade e dos direitos e liberdades fundamentais dos indivíduos para a transferência, pelo Exportador de Dados ao Importador de Dados, dos Dados Pessoais especificados no Anexo 1.

Estas Cláusulas estabelecem salvaguardas apropriadas, incluindo direitos executáveis do titular dos dados e recursos legais eficazes, de acordo com o Artigo 46(1) e Artigo 46 (2)(c) do GDPR e, com relação às transferências de dados de controladores para processadores e/ou processadores para processadores, cláusulas contratuais padrão de acordo com o Artigo 28(7) do GDPR, desde que não sejam modificadas, exceto para adicionar ou atualizar informações nos Anexos. Isso não impede que as Partes incluam as cláusulas contratuais padrão estabelecidas nestas Cláusulas em um contrato mais amplo e acrescentem outras cláusulas ou garantias adicionais, desde que não contradigam, direta ou indiretamente, as cláusulas contratuais padrão ou prejudiquem os direitos ou liberdades fundamentais dos titulares dos dados. Estas Cláusulas não prejudicam as obrigações às quais o exportador de dados está sujeito em virtude do GDPR.

Estas Cláusulas se aplicam com relação à transferência de dados pessoais, conforme especificado na Cláusula 2.

Cláusula 1

Definições

1.1. Os termos definidos abaixo terão o mesmo significado que no GDPR; os termos, portanto, deverão ser lidos e interpretados à luz das disposições do GDPR

a) "dados pessoais", "categorias especiais de dados", "processamento/tratamento", "controlador", "processador", "titular dos dados" e "autoridade supervisora" terão o mesmo significado que na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

b) "Exportador de dados" significa o controlador que transfere os dados pessoais;

c) "o Importador de Dados" significa o Processador que concorda em receber do Exportador de Dados os Dados Pessoais destinados ao processamento em seu nome após a transferência, de acordo com suas instruções e com os termos das Cláusulas, e que não está sujeito a um sistema de um terceiro país que garanta a proteção adequada no sentido do Artigo 25(1) da Diretiva 95/46/EC;

d) "o subprocessador" significa qualquer processador contratado pelo Importador de dados ou por qualquer outro subprocessador do Importador de dados que concorde em receber do Importador de dados ou de qualquer outro subprocessador do Importador de dados os Dados pessoais destinados exclusivamente a atividades de processamento a serem realizadas em nome do Exportador de dados após a transferência, de acordo com suas instruções, os termos das Cláusulas e os termos do subcontrato por escrito;

e) "a lei de proteção de dados aplicável" significa a legislação que protege os direitos e liberdades fundamentais dos indivíduos e, em particular, seu direito à privacidade com relação ao Processamento de Dados Pessoais aplicável a um Controlador de Dados no Estado Membro no qual o Exportador de Dados está estabelecido;

f) "medidas de segurança técnicas e organizacionais" significa as medidas destinadas a proteger os dados pessoais contra destruição acidental ou ilegal ou perda acidental, alteração, divulgação ou acesso não autorizado, em particular quando o processamento envolver

a transmissão de dados por uma rede, e contra todas as outras formas ilegais de processamento.

1.2 Estas Cláusulas não devem ser interpretadas de forma que entrem em conflito com os direitos e obrigações previstos no GDPR.

Cláusula 2

Detalhes da transferência

Os detalhes da transferência e, em particular, as categorias especiais de Dados Pessoais que são transferidos e as finalidades para as quais são transferidos, estão especificados no Anexo 1, que é parte integrante das Cláusulas.

Cláusula 3

Cláusula do terceiro beneficiário

3.1 Os titulares de dados podem invocar e aplicar estas Cláusulas, como terceiros beneficiários, contra o exportador e/ou importador de dados, com as seguintes exceções:

- (i) Cláusulas relativas à finalidade e ao escopo, terceiros beneficiários, definição, hierarquia e descrição da transferência
- (ii) Cláusula sobre a conformidade da documentação
- (iii) Cláusula sobre notificação
- (iv) Cláusula relativa ao uso de subprocessador
- (v) Cláusula relativa à responsabilidade;
- (vi) Cláusula de indenização;
- (vii) Cláusula de supervisão;
- (viii) Cláusulas de não conformidade e jurisdição i.

Cláusula 4

Obrigações do exportador de dados

O exportador de dados garante que envidou esforços razoáveis para determinar que o importador de dados é capaz de cumprir suas obrigações nos termos desta Cláusula como salvaguarda:

4.1. que o processamento, incluindo a própria transferência, dos Dados Pessoais foi e continuará a ser realizado de acordo com as disposições relevantes da lei de proteção de dados aplicável (e, quando aplicável, foi notificado às autoridades relevantes do Estado Membro onde o Exportador de Dados está estabelecido) e não viola as disposições relevantes desse Estado;

4.2. que instruiu e, durante toda a duração dos serviços de processamento de Dados Pessoais, instruirá o Importador de Dados a processar os Dados Pessoais transferidos somente em nome do Exportador de Dados e de acordo com a lei de proteção de dados aplicável e as Cláusulas, e que o Importador de Dados processará os dados pessoais somente para a(s) finalidade(s) específica(s) da transferência, conforme estabelecido no Anexo 1.

4.3. que o Importador de Dados fornecerá garantias suficientes com relação às medidas de segurança técnicas e organizacionais especificadas no Apêndice 2 deste contrato;

4.4. que, após a avaliação dos requisitos da lei de proteção de dados aplicável, as medidas de segurança são adequadas para proteger os Dados Pessoais contra destruição acidental ou ilegal ou perda acidental, alteração, divulgação ou acesso não autorizado, em particular quando o processamento envolver a transmissão de dados por uma rede, e contra todas as outras formas ilegais de processamento, e que essas medidas garantem um nível de segurança adequado aos riscos apresentados pelo processamento e à natureza dos dados a serem protegidos, considerando o estado da arte e o custo de sua implementação;

4.5. que garantirá a conformidade com as medidas de segurança;

4.6. que, se a transferência envolver categorias especiais de dados, o Titular dos Dados foi informado ou será informado antes, ou o mais rápido possível após a transferência, de que seus dados podem ser transmitidos a um terceiro país que não oferece proteção adequada no sentido do GDPR;

4.7. encaminhar qualquer notificação recebida do Importador de Dados ou de qualquer subprocessador nos termos da Cláusula 5(b) e da Cláusula 8(3) à autoridade supervisora de proteção de dados se o Exportador de Dados decidir continuar a transferência ou suspender a suspensão;

4.8. disponibilizar aos Titulares dos Dados, mediante solicitação, uma cópia das Cláusulas, com exceção do Apêndice 2, e uma descrição resumida das medidas de segurança, bem como uma cópia de qualquer contrato para serviços de subprocessamento que tenha que ser feito de acordo com as Cláusulas, a menos que as Cláusulas ou o contrato contenham informações comerciais, caso em

que poderá remover tais informações comerciais;

4.9. que, no caso de subprocessamento, a atividade de processamento seja realizada de acordo com a Cláusula 11 por um subprocessador que forneça, no mínimo, o mesmo nível de proteção para os dados pessoais e os direitos do titular dos dados que o Importador de Dados de acordo com as Cláusulas; e

4.10. que garantirá a conformidade com a Cláusula 4(a) a (i)

4.11. Não apenas o exportador de dados, mas também o importador de dados deverá fornecer ao titular dos dados uma cópia das cláusulas mediante solicitação. Na medida do necessário para proteger segredos comerciais ou outras informações confidenciais, incluindo as medidas descritas no Apêndice II, as Partes poderão redigir o texto dos Apêndices destas Cláusulas antes de compartilhar uma cópia, mas deverão fornecer um resumo significativo quando, de outra forma, o titular dos dados não seria capaz de compreender o conteúdo dos Apêndices. Isso não obstante as obrigações do exportador de dados nos termos dos artigos 13 e 14 do GDPR, em particular para informar o titular dos dados sobre a transferência de categorias especiais de dados.

Cláusula 5

Obrigações do importador de dados

O Importador de dados concorda e garante:

5.1. processar os Dados Pessoais somente em nome do Exportador de Dados e em conformidade com suas instruções e com as Cláusulas; se não puder fornecer essa conformidade por qualquer motivo, concorda em informar imediatamente o Exportador de Dados sobre sua incapacidade de cumprir, caso em que o Exportador de Dados tem o direito de suspender a transferência de dados e/ou rescindir o contrato;

5.2. processar os dados pessoais somente para a(s) finalidade(s) específica(s) da transferência, conforme estabelecido no Anexo 1.

5.3. que, se o importador de dados tomar conhecimento de que os dados pessoais que recebeu são imprecisos ou estão desatualizados, ele deverá informar o exportador de dados sem atrasos indevidos. Nesse caso, o importador de dados deverá cooperar com o exportador de dados para apagar ou retificar os dados.

5.4. que o processamento pelo importador de dados somente ocorrerá durante o período especificado no Apêndice 1. Após o término da prestação dos serviços de processamento, o importador de dados deverá, a critério do exportador de dados, excluir todos os dados pessoais processados em nome do exportador de dados e certificar ao exportador de dados que o fez, ou devolver ao exportador de dados todos os dados pessoais processados em seu nome e excluir as cópias existentes. Até que os dados sejam excluídos ou devolvidos, o importador de dados deverá continuar a garantir a conformidade com estas Cláusulas. No caso de leis locais aplicáveis ao importador de dados que proíbam a devolução ou a exclusão dos dados pessoais, o importador de dados garante que continuará a garantir a conformidade com estas Cláusulas e que somente os processará na medida e pelo tempo exigidos pela lei local. Isso não prejudica a exigência de que o importador de dados notifique o exportador de dados durante toda a vigência do contrato se tiver motivos para acreditar que está ou se tornou sujeito a leis ou práticas que não estejam de acordo com as exigências do GDPR.

5.5. que o importador de dados concederá acesso aos dados pessoais a membros de sua equipe somente na medida estritamente necessária para a implementação, gerenciamento e monitoramento do contrato. Ele deverá garantir que as pessoas autorizadas a processar os dados pessoais tenham se comprometido com a confidencialidade ou estejam sob uma obrigação legal apropriada de confidencialidade.

5.6. que, no caso de uma violação de dados pessoais relativa a dados pessoais processados pelo importador de dados de acordo com estas Cláusulas, o importador de dados tomará as medidas adequadas para resolver a violação, inclusive medidas para mitigar seus efeitos adversos. O importador de dados também notificará o exportador de dados sem atrasos indevidos após ter tomado conhecimento da violação. Essa notificação deve conter os detalhes de um ponto de contato onde mais informações possam ser obtidas, uma descrição da natureza da violação (incluindo, quando possível, as categorias e o número aproximado de titulares de dados e registros de dados pessoais em questão), suas consequências prováveis e as medidas tomadas ou propostas para solucionar a violação, incluindo, quando apropriado, medidas para atenuar seus possíveis efeitos adversos. Quando, e na medida em que, não for possível fornecer todas as informações ao mesmo tempo, a notificação inicial deverá conter as informações disponíveis no momento e outras informações deverão ser fornecidas posteriormente, à medida que estiverem disponíveis, sem atrasos indevidos.

5.7. que, quando a transferência envolver dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical, dados genéticos ou dados biométricos para fins de identificação exclusiva de uma pessoa física, dados relativos à saúde ou à vida sexual ou orientação sexual de uma pessoa, ou dados relativos a condenações penais e infrações (doravante denominados "dados sensíveis"), o importador de dados deverá aplicar as restrições específicas e/ou garantias adicionais descritas no

Apêndice 2.

5.8. que o importador de dados somente divulgará os dados pessoais a um terceiro mediante instruções documentadas do exportador de dados. Além disso, os dados somente poderão ser divulgados a um terceiro localizado fora da União Europeia (4) (no mesmo país que o importador de dados ou em outro país terceiro, doravante denominada "transferência subsequente") se o terceiro estiver ou concordar em se vincular a estas Cláusulas, sob o Módulo apropriado, ou se:

(i) a transferência subsequente é para um país que se beneficia de uma decisão de adequação nos termos do artigo 45 do Regulamento (UE) 2016/679 que abrange a transferência subsequente;

(ii) o terceiro garante de outra forma as salvaguardas apropriadas de acordo com os artigos 46 ou 47 do Regulamento (UE) 2016/679 com relação ao processamento em questão;

(iii) a transferência subsequente é necessária para o estabelecimento, exercício ou defesa de reivindicações legais no contexto de procedimentos administrativos, regulatórios ou judiciais específicos; ou

(iv) a transferência subsequente é necessária para proteger os interesses vitais do titular dos dados ou de outra pessoa física.

Qualquer transferência subsequente está sujeita à conformidade do importador de dados com todas as outras proteções previstas nestas Cláusulas, em especial a limitação de finalidade.

5.9. que o importador de dados deve informar aos titulares de dados, de forma transparente e facilmente acessível, por meio de aviso individual ou em seu site, sobre um ponto de contato autorizado a lidar com reclamações. Ele deverá tratar prontamente quaisquer reclamações que receber de um titular de dados.

5.10. que não tem motivos para acreditar que a legislação aplicável a ela a impeça de cumprir as instruções recebidas do Exportador de dados e suas obrigações nos termos do contrato e que, no caso de uma alteração nessa legislação que possa ter um efeito adverso substancial sobre as garantias e obrigações previstas nas Cláusulas, ela notificará imediatamente a alteração ao Exportador de dados assim que tiver conhecimento, caso em que o Exportador de dados terá o direito de suspender a transferência de dados e/ou rescindir o contrato;

5.11. que implementou as medidas de segurança técnicas e organizacionais especificadas no Anexo 2 antes de processar os Dados Pessoais transferidos;

5.12. que notificará prontamente o exportador de dados sobre:

i. qualquer solicitação legalmente vinculativa de divulgação dos dados pessoais por uma autoridade de aplicação da lei, a menos que seja proibido de outra forma, como uma proibição sob a lei criminal para preservar a confidencialidade de uma investigação de aplicação da lei,

ii. qualquer acesso acidental ou não autorizado, e

iii. qualquer solicitação recebida diretamente dos titulares dos dados sem responder a essa solicitação, a menos que tenha sido autorizado a fazê-lo de outra forma;

5.13. que o importador de dados ajudará o exportador de dados a cumprir suas obrigações de responder às solicitações dos titulares de dados para o exercício de seus direitos nos termos do Regulamento (UE) 2016/679. Nesse sentido, as Partes estabelecerão no Apêndice II as medidas técnicas e organizacionais adequadas, levando em conta a natureza do processamento, por meio das quais a assistência será prestada, bem como o escopo e a extensão da assistência necessária.

5.14. lidar pronta e adequadamente com todas as consultas do exportador de dados relacionadas ao seu processamento dos dados pessoais sujeitos à transferência e acatar a orientação da autoridade supervisora com relação ao processamento dos dados transferidos;

5.15. a pedido do Exportador de dados, submeter suas instalações de processamento de dados para auditoria das atividades de processamento cobertas pelas Cláusulas, que será realizada pelo Exportador de dados ou por um órgão de inspeção composto por membros independentes e que possuam as qualificações profissionais exigidas, vinculados a um dever de confidencialidade, selecionado pelo Exportador de dados, quando aplicável, de acordo com a autoridade supervisora;

5.16. o exportador de dados poderá optar por realizar a auditoria sozinho ou solicitar um auditor independente. As auditorias podem incluir inspeções nas dependências ou instalações físicas do importador de dados e devem, quando apropriado, ser realizadas com aviso prévio razoável.

5.17. que o importador de dados manterá a documentação adequada sobre as atividades de processamento realizadas em nome do exportador de dados.

5.18. disponibilizar ao Titular dos Dados, mediante solicitação, uma cópia das Cláusulas ou de qualquer contrato existente para subprocessamento, a menos que as Cláusulas ou o contrato contenham informações comerciais, caso em que poderá remover essas informações comerciais, com exceção do Apêndice 2, que deverá ser substituído por uma descrição resumida das medidas de

segurança nos casos em que o Titular dos Dados não puder obter uma cópia do Exportador de Dados;

5.19. que, no caso de subprocessamento, tenha informado previamente o Exportador de Dados e obtido seu consentimento prévio por escrito;

5.20. que os serviços de processamento pelo subprocessador serão executados de acordo com a Cláusula 11;

5.21. enviar prontamente ao Exportador de Dados uma cópia de qualquer contrato de subprocessador celebrado nos termos das Cláusulas.

5.22. Cooperar de boa-fé e auxiliar o exportador de dados de qualquer forma necessária para permitir que o exportador de dados cumpra suas obrigações de acordo com o GDPR, principalmente para notificar a autoridade supervisora competente e os titulares de dados afetados, levando em consideração a natureza do processamento e as informações disponíveis para o importador de dados.

Cláusula 6

Responsabilidade civil

6.1. As partes concordam que qualquer Titular de Dados que tenha sofrido danos como resultado de qualquer violação das obrigações mencionadas na Cláusula 3 ou na Cláusula 11 por qualquer parte ou subprocessador tem o direito de receber uma indenização do Exportador de Dados pelos danos sofridos.

6.2. Cada Parte será responsável perante a(s) outra(s) Parte(s) por quaisquer danos materiais ou imateriais que causar(em) à(s) outra(s) Parte(s) por qualquer violação destas Cláusulas. A responsabilidade entre as Partes é limitada aos danos efetivamente sofridos. Os danos punitivos estão excluídos.

6.3. O importador de dados será responsável perante o titular dos dados, e o titular dos dados terá o direito de receber indenização, por quaisquer danos materiais ou morais que o importador de dados ou seu subprocessador causar ao titular dos dados por violar os direitos de terceiros beneficiários nos termos destas Cláusulas.

6.4. As Partes concordam que, se o exportador de dados for considerado responsável por danos causados pelo importador de dados (ou seu subprocessador), ele terá o direito de reivindicar do importador de dados a parte da indenização correspondente à responsabilidade do importador de dados pelo dano.

6.5. Quando mais de uma Parte for responsável por qualquer dano causado ao titular dos dados como resultado de uma violação destas Cláusulas, todas as Partes responsáveis serão conjunta e solidariamente responsáveis e o titular dos dados terá o direito de mover uma ação judicial contra qualquer uma dessas Partes. As Partes concordam que, se uma Parte for considerada responsável, ela terá o direito de reivindicar da(s) outra(s) Parte(s) a parte da indenização correspondente à sua responsabilidade pelo dano.

6.6. O importador de dados não poderá invocar a conduta de um subprocessador para evitar sua própria responsabilidade.

6.7. Se um Titular de Dados não puder apresentar um pedido de indenização de acordo com o parágrafo 1 contra o Exportador de Dados, decorrente de uma violação pelo Importador de Dados ou seu subprocessador de qualquer uma de suas obrigações mencionadas na Cláusula 3 ou na Cláusula 11, porque o Exportador de Dados desapareceu de fato ou deixou de existir legalmente ou se tornou insolvente, o Importador de Dados concorda que o Titular dos Dados poderá emitir uma reivindicação contra o Importador de Dados como se fosse o Exportador de Dados, a menos que qualquer entidade sucessora tenha assumido todas as obrigações legais do Exportador de Dados por contrato ou por força de lei, caso em que o Titular dos Dados poderá fazer valer seus direitos contra essa entidade.

6.8. O Importador de dados não poderá se basear em uma violação de suas obrigações por um subprocessador para evitar suas próprias responsabilidades e não poderá invocar a conduta de um subprocessador

6.9. Se um Titular dos Dados não puder apresentar uma reivindicação contra o Exportador ou Importador de Dados mencionado nos parágrafos 1 e 2, decorrente de uma violação pelo subprocessador de qualquer uma de suas obrigações mencionadas na Cláusula 3 ou na Cláusula 11, porque tanto o Exportador quanto o Importador de Dados desapareceram de fato ou deixaram de existir legalmente ou se tornaram insolventes, o subprocessador concorda que o Titular dos Dados poderá apresentar uma reclamação contra o subprocessador de dados com relação às suas próprias operações de processamento nos termos das Cláusulas como se fosse o Exportador ou Importador de Dados, a menos que qualquer entidade sucessora tenha assumido todas as obrigações legais do Exportador ou Importador de Dados por contrato ou por força de lei, caso em que o Titular dos Dados poderá fazer valer seus direitos contra essa entidade. A responsabilidade do subprocessador será limitada às suas próprias operações de processamento nos termos das Cláusulas.

6.10. Em caso de controvérsia entre um titular de dados e uma das Partes no que diz respeito ao cumprimento destas Cláusulas, a Parte deverá envidar seus melhores esforços para resolver a questão de forma amigável e em tempo hábil. As Partes deverão manter-se

mutuamente informadas sobre tais disputas e, quando apropriado, cooperar para resolvê-las.

6.11. Quando o titular dos dados invocar um direito de terceiro beneficiário nos termos da Cláusula 3, o importador de dados deverá aceitar a decisão do titular dos dados de:

- (i) apresentar uma reclamação à autoridade supervisora do Estado Membro de sua residência habitual ou local de trabalho, ou à autoridade supervisora competente;
- (ii) encaminhar a disputa para os tribunais competentes.

6.12. As Partes aceitam que o titular dos dados pode ser representado por um órgão, organização ou associação sem fins lucrativos nas condições estabelecidas no Artigo 80(1) do Regulamento (UE) 2016/679.

6.13. O importador de dados deverá cumprir uma decisão que seja vinculante de acordo com a legislação aplicável da UE ou do Estado Membro.

6.14. O importador de dados concorda que a escolha feita pelo titular dos dados não prejudicará seus direitos substantivos e processuais de buscar soluções de acordo com as leis aplicáveis.

Cláusula 7

Mediação e jurisdição

7.1. O Importador de dados concorda que, se o titular dos dados invocar contra ele direitos de terceiros beneficiários e/ou solicitar indenização por danos nos termos das Cláusulas, o Importador de dados aceitará a decisão do titular dos dados:

- i. encaminhar a disputa para mediação, por uma pessoa independente ou, quando aplicável, pela autoridade supervisora;
- ii. encaminhar a disputa para os tribunais do Estado Membro no qual o Exportador de dados está estabelecido.

As Partes concordam que a escolha feita pelo Titular dos Dados não prejudicará seus direitos substantivos ou processuais de buscar soluções de acordo com outras disposições da legislação nacional ou internacional.

Cláusula 8

Cooperação com autoridades de supervisão

8.1. O exportador de dados concorda em depositar uma cópia deste contrato com a autoridade supervisora, se ela assim o solicitar ou se tal depósito for exigido pela lei de proteção de dados aplicável.

8.2. As partes concordam que a autoridade supervisora tem o direito de conduzir uma auditoria do Importador de dados e de qualquer subprocessador, que tem o mesmo escopo e está sujeita às mesmas condições que se aplicariam a uma auditoria do Exportador de dados de acordo com a lei de proteção de dados aplicável.

8.3. O Importador de Dados informará imediatamente o Exportador de Dados sobre a existência de legislação aplicável a ele ou a qualquer subprocessador que impeça a realização de uma auditoria do Importador de Dados, ou de qualquer subprocessador, nos termos do parágrafo 2. Em tal caso, o Exportador de Dados terá o direito de tomar as medidas previstas na Cláusula 5 (b).

Cláusula 9

Legislação aplicável e escolha do foro

9.1. As Cláusulas serão regidas pela legislação do Estado Membro em que o Exportador de Dados estiver estabelecido. Quando essa lei não permitir direitos de terceiros beneficiários, elas serão regidas pela lei de outro Estado Membro da UE que permita direitos de terceiros beneficiários.

9.2. Qualquer controvérsia decorrente destas Cláusulas deverá ser resolvida pelos tribunais de um Estado Membro da UE.

9.3. O titular dos dados também pode mover uma ação judicial contra o exportador e/ou importador de dados perante os tribunais do Estado Membro em que tem sua residência habitual.

9.4. As Partes concordam em se submeter à jurisdição de tais tribunais.

Cláusula 10

Variação do contrato

As partes se comprometem a não variar ou modificar as Cláusulas. Isso não impede que as partes acrescentem cláusulas sobre questões relacionadas aos negócios, quando necessário, desde que não contradigam a Cláusula.

Cláusula 11

Subprocessamento

11.1. O Importador de dados não subcontratará nenhuma de suas operações de processamento realizadas em nome do Exportador de dados nos termos das Cláusulas sem o consentimento prévio por escrito do Exportador de dados. O importador de dados deverá enviar a solicitação de autorização específica pelo menos [Especificar o período de tempo] antes da contratação do subprocessador, juntamente com as informações necessárias para permitir que o exportador de dados decida sobre a autorização. Quando o Importador de dados subcontratar suas obrigações nos termos das Cláusulas, com o consentimento do Exportador de dados, ele deverá fazê-lo somente por meio de um contrato por escrito com o subprocessador que imponha ao subprocessador as mesmas obrigações impostas ao Importador de dados nos termos das Cláusulas. Caso o subprocessador não cumpra suas obrigações de proteção de dados nos termos do referido contrato por escrito, o Importador de dados permanecerá totalmente responsável perante o Exportador de dados pelo cumprimento das obrigações do subprocessador nos termos do referido contrato.

11.2. O contrato prévio por escrito entre o Importador de dados e o subprocessador também deverá prever uma cláusula de terceiro beneficiário, conforme estabelecido na Cláusula 3, para os casos em que o titular dos dados não puder apresentar o pedido de indenização referido no parágrafo 1 da Cláusula 6 contra o Exportador de dados ou o Importador de dados porque eles desapareceram de fato ou deixaram de existir legalmente ou se tornaram insolventes e nenhuma entidade sucessora assumiu todas as obrigações legais do Exportador de dados ou do Importador de dados por contrato ou por força de lei. Essa responsabilidade de terceiros do subprocessador será limitada às suas próprias operações de processamento nos termos das Cláusulas.

11.3. As disposições relacionadas aos aspectos de proteção de dados para o subprocessamento do contrato mencionado no parágrafo 1 serão regidas pela lei do Estado Membro no qual o exportador de dados está estabelecido.

11.4. O Exportador de dados manterá uma lista dos acordos de subprocessamento celebrados nos termos das Cláusulas e notificados pelo Importador de dados nos termos da Cláusula 5(j), que será atualizada pelo menos uma vez por ano. A lista deverá estar disponível para a autoridade supervisora de proteção de dados do Exportador de Dados.

11.5. O importador de dados deverá fornecer, mediante solicitação do exportador de dados ou do controlador, uma cópia desse contrato de subprocessador e das alterações subsequentes.

11.6. O importador de dados permanecerá totalmente responsável perante o exportador de dados pelo cumprimento das obrigações do subprocessador nos termos de seu contrato com o importador de dados. O importador de dados notificará o exportador de dados sobre qualquer falha do subprocessador em cumprir suas obrigações nos termos desse contrato.

11.7. O importador de dados acordará uma cláusula de terceiro beneficiário com o subprocessador, segundo a qual, em caso de falência do importador de dados, o exportador de dados será um terceiro beneficiário do contrato do subprocessador e terá o direito de executar o contrato contra o subprocessador, inclusive, quando aplicável, instruindo o subprocessador a apagar ou devolver os dados pessoais.

Cláusula 12

Obrigação após o término dos serviços de processamento de dados pessoais

12.1. As partes concordam que, ao término da prestação de serviços de processamento de dados, o Importador de dados e o subprocessador deverão, a critério do Exportador de dados, devolver todos os dados pessoais transferidos e suas cópias ao Exportador de dados ou destruir todos os dados pessoais e certificar ao Exportador de dados que o fizeram, a menos que a legislação imposta ao Importador de dados o impeça de devolver ou destruir todos ou parte dos dados pessoais transferidos. Nesse caso, o Importador de dados garante que garantirá a confidencialidade dos dados pessoais transferidos e não processará mais ativamente os dados pessoais transferidos.

Cláusula 13

Hierarquia

Em caso de conflito entre estas Cláusulas e as disposições de qualquer outro contrato entre as Partes existente no momento em que estas Cláusulas forem acordadas ou celebradas posteriormente, estas Cláusulas prevalecerão.

Cláusula 14

Leis locais que afetam a conformidade com as Cláusulas

14.1. As Partes garantem que não têm motivos para acreditar que as leis do terceiro país de destino aplicáveis ao processamento dos dados pessoais pelo importador de dados, incluindo quaisquer requisitos de divulgação de dados pessoais ou medidas que autorizem o

acesso por autoridades públicas, impeçam o importador de dados de cumprir suas obrigações nos termos destas Cláusulas. Isso se baseia no entendimento de que as leis que respeitam a essência dos direitos e liberdades fundamentais e não excedem o que é necessário e proporcional em uma sociedade democrática para salvaguardar um dos objetivos listados no Artigo 23(1) do GDPR não estão em contradição com as Cláusulas.

14.2. As Partes declaram que, ao fornecer a garantia prevista no Artigo 14.1, elas levaram em consideração, em especial, os seguintes elementos: (i) as circunstâncias específicas da transferência, incluindo o conteúdo e a duração do contrato; a escala e a regularidade das transferências; a extensão da cadeia de processamento, o número de atores envolvidos e os canais de transmissão utilizados; o tipo de destinatário; a finalidade do processamento; a natureza dos dados pessoais transferidos; qualquer experiência prática relevante com instâncias anteriores, ou a ausência de solicitações de divulgação de autoridades públicas recebidas pelo importador de dados para o tipo de dados transferidos; (ii) as leis do terceiro país de destino relevantes à luz das circunstâncias da transferência, incluindo aquelas que exigem a divulgação de dados a autoridades públicas ou que autorizam o acesso por tais autoridades, bem como as limitações e salvaguardas aplicáveis; (iii) quaisquer salvaguardas além daquelas previstas nestas Cláusulas, incluindo as medidas técnicas e organizacionais aplicadas durante a transmissão e ao processamento dos dados pessoais no país de destino.

14.3. O importador de dados garante que, ao realizar a avaliação nos termos do Artigo 14.2, envidou seus melhores esforços para fornecer ao exportador de dados as informações relevantes e concorda que continuará a cooperar com o exportador de dados para garantir a conformidade com estas Cláusulas.

Cláusula 15

Obrigações do importador de dados em caso de solicitações de acesso do governo

15.1 Notificação

15.1.1. O importador de dados concorda em notificar prontamente o exportador de dados e, quando possível, o titular dos dados (se necessário, com a ajuda do exportador de dados) se ele: (i) receber uma solicitação legalmente vinculante de uma autoridade pública nos termos das leis do país de destino para a divulgação de dados pessoais transferidos de acordo com estas Cláusulas; tal notificação deverá incluir informações sobre os dados pessoais solicitados, a autoridade solicitante, a base legal para a solicitação e a resposta fornecida; PT 15 PT (ii) tomar conhecimento de qualquer acesso direto por autoridades públicas a dados pessoais transferidos de acordo com estas Cláusulas, nos termos das leis do país de destino; tal notificação deverá incluir todas as informações disponíveis para o importador.

15.1.2. Se o importador de dados for proibido de notificar o exportador de dados e/ou o titular dos dados, o importador de dados concorda em envidar seus melhores esforços para obter uma isenção da proibição, com o objetivo de comunicar o máximo de informações e o mais rápido possível. O importador de dados concorda em documentar seus melhores esforços a fim de poder demonstrá-los mediante solicitação do exportador de dados.

15.1.3. Na medida do permitido pelas leis do país de destino, o importador de dados concorda em fornecer ao exportador de dados, em intervalos regulares durante a vigência do contrato, a maior quantidade possível de informações relevantes sobre as solicitações recebidas (em particular, número de solicitações, tipo de dados solicitados, autoridade ou autoridades solicitantes, se as solicitações foram contestadas e o resultado de tais contestações, etc.).

15.1.4. O importador de dados concorda em preservar as informações de acordo com os Artigos 15.1.1 a 15.1.3 durante a vigência do contrato e disponibilizá-las à autoridade supervisora competente mediante solicitação.

15.1.5. Os artigos 15.1.1 a 15.1.3 não se aplicam à obrigação do importador de dados, de acordo com a cláusula de rescisão, de informar prontamente o exportador de dados quando não puder cumprir estas Cláusulas.

15.2 Revisão da legalidade e minimização de dados

15.2.1. O importador de dados concorda em analisar, de acordo com as leis do país de destino, a legalidade da solicitação de divulgação, notadamente se ela está dentro dos poderes concedidos à autoridade pública solicitante, e em esgotar todos os recursos disponíveis para contestar a solicitação se, após uma avaliação cuidadosa, concluir que há motivos para fazê-lo de acordo com as leis do país de destino. Ao contestar uma solicitação, o importador de dados deverá buscar medidas provisórias com o objetivo de suspender os efeitos da solicitação até que o tribunal decida sobre o mérito. Ele não divulgará os dados pessoais solicitados até que seja solicitado a fazê-lo de acordo com as regras processuais aplicáveis. Esses requisitos não se aplicam às obrigações do importador de dados de acordo com o Artigo 15.1.5.

15.2.2. O importador de dados concorda em documentar sua avaliação jurídica, bem como qualquer contestação à solicitação de divulgação e, na medida do permitido pelas leis do país de destino, disponibilizá-la ao exportador de dados. Ele também deverá

disponibilizá-la à autoridade supervisora competente mediante solicitação.

15.2.3. O importador de dados concorda em fornecer a quantidade mínima de informações permitida ao responder a uma solicitação de divulgação, com base em uma interpretação razoável da solicitação

Cláusula 16

Não conformidade com as Cláusulas e rescisão

16.1. O importador de dados deverá informar prontamente o exportador de dados se não puder cumprir essas Cláusulas, por qualquer motivo.

16.2. Caso o importador de dados esteja violando estas Cláusulas ou seja incapaz de cumpri-las, o exportador de dados suspenderá a transferência de dados pessoais para o importador de dados até que a conformidade seja novamente assegurada ou o contrato seja rescindido.

16.3. O exportador de dados terá o direito de rescindir o contrato, no que diz respeito ao processamento de dados pessoais nos termos destas Cláusulas, quando

(i) o exportador de dados tiver suspenso a transferência de dados pessoais para o importador de dados nos termos do parágrafo (b) e a conformidade com estas Cláusulas não for restabelecida dentro de um prazo razoável e, em qualquer caso, dentro de um mês após a suspensão;

(ii) o importador de dados estiver em violação substancial ou persistente destas Cláusulas; ou

(iii) o importador de dados deixar de cumprir uma decisão vinculante de um tribunal competente ou de uma autoridade supervisora com relação às suas obrigações nos termos destas Cláusulas.

Nesses casos, ele deverá informar a autoridade supervisora competente [para o Módulo Três: e o controlador] sobre essa não conformidade. Quando o contrato envolver mais de duas Partes, o exportador de dados poderá exercer esse direito de rescisão somente com relação à Parte relevante, a menos que as Partes tenham acordado de outra forma.

16.4. Os dados pessoais que tenham sido transferidos antes da rescisão do contrato nos termos do Artigo 16.3 deverão, a critério do exportador de dados, ser imediatamente devolvidos ao exportador de dados ou excluídos em sua totalidade. O mesmo se aplicará a quaisquer cópias dos dados. O importador de dados deverá certificar a exclusão dos dados ao exportador de dados. Até que os dados sejam excluídos ou devolvidos, o importador de dados deverá continuar a garantir a conformidade com estas Cláusulas. No caso de leis locais aplicáveis ao importador de dados que proíbam a devolução ou a exclusão dos dados pessoais transferidos, o importador de dados garante que continuará a garantir a conformidade com estas Cláusulas e que somente processará os dados na medida e pelo tempo exigidos pela lei local.

16.5. Qualquer uma das Partes poderá revogar seu acordo de vinculação a estas Cláusulas quando (i) a Comissão Europeia adotar uma decisão nos termos do Artigo 45(3) do Regulamento (UE) 2016/679 que abranja a transferência de dados pessoais aos quais estas Cláusulas se aplicam; ou (ii) o Regulamento (UE) 2016/679 se tornar parte da estrutura jurídica do país para o qual os dados pessoais são transferidos. Isso não prejudica outras obrigações aplicáveis ao processamento em questão nos termos do Regulamento (UE) 2016/679.

Cláusula 17

Cláusula de ancoragem

17.1. Uma entidade que não seja uma Parte destas Cláusulas poderá, com o acordo das Partes, aderir a estas Cláusulas a qualquer momento, seja como exportador de dados ou como importador de dados, mediante preencher o Apêndice e assinar o Anexo I.A.

17.2. Uma vez preenchido o Apêndice e assinado o Anexo I.A, a entidade aderente deverá tornar-se uma Parte destas Cláusulas e ter os direitos e as obrigações de um usuário de dados exportador ou importador de dados, de acordo com sua designação no Anexo I.A.

17.3. A entidade aderente não terá direitos ou obrigações decorrentes destas Cláusulas do período anterior a se tornar uma Parte.

Em nome do exportador de dados:

Nome (escrito por extenso):

Posição:

Endereço:

Outras informações necessárias para que o contrato seja vinculativo (se houver):

Assinatura:

Em nome do importador de dados:

Nome (escrito por extenso):

Posição:

Endereço:

Outras informações necessárias para que o contrato seja vinculativo (se houver):

Assinatura:

Apêndice 1

Este Apêndice faz parte das Cláusulas e deve ser preenchido e assinado pelas partes. Os Estados Membros podem completar ou especificar, de acordo com seus procedimentos nacionais, quaisquer informações adicionais necessárias a serem incluídas neste Apêndice.

Exportador de dados

O tipo de negócio ou organização do exportador de dados é (especifique brevemente suas atividades relevantes para a transferência):

Governo central

Caritativo e voluntário

Educação e cuidados infantis

Finanças, seguros e crédito

Negócios gerais

Saúde

TI, digital, tecnologia e telecomunicações

Justiça e policiamento

Serviços de terrenos e propriedades

Consultores jurídicos e profissionais

Governo local

Marketing e pesquisa

Mídia

Associação de membros

Política

Reguladores

Religioso

Pesquisa

Varejo e manufatura

Assistência social

Associações comerciais, de empregadores e órgãos profissionais

Comerciantes de dados pessoais

Transporte e lazer

Serviços públicos e recursos naturais

Outro - Adicione detalhes:

O exportador de dados está usando os dados pessoais que estão sendo transferidos para as seguintes finalidades ou atividades:

Atividades comerciais padrão, que se aplicam à maioria das empresas e organizações

Administração de pessoal, inclusive pessoal permanente e temporário, incluindo nomeação ou remoção, pagamento, disciplina, aposentadoria, gerenciamento de trabalho e outros assuntos de pessoal em relação à equipe do exportador de dados.

Publicidade, marketing e relações públicas do próprio negócio ou atividade, bens ou serviços do exportador de dados.

Contas e registros, incluindo

- manter contas relacionadas ao negócio ou à atividade do exportador de dados;

- decidir se aceitará qualquer pessoa ou organização como cliente;

- manter registros de compras, vendas ou outras transações, incluindo pagamentos, entregas ou serviços fornecidos pelo exportador de dados ou para o exportador de dados;

- manter registros de clientes

- registros para fazer previsões financeiras ou gerenciais; e

- outras atividades gerais de manutenção de registros e gerenciamento de informações.

Outras atividades:

Serviços de contabilidade e auditoria

Administração da justiça, incluindo a administração interna e o gerenciamento de tribunais ou cortes e o cumprimento de tarefas judiciais.

Administração de registros de associados ou apoiadores.

Propaganda, marketing e relações públicas para terceiros, inclusive trabalho de relações públicas, propaganda e marketing, envio de correspondências para outras organizações e corretagem de listas.

Avaliação e cobrança de impostos, taxas, tributos e outras receitas

Administração de benefícios, bem-estar, subsídios e empréstimos

Prospecção, busca e manutenção de apoio político entre o eleitorado.

Trabalho de caso do distrito eleitoral em nome de constituintes individuais por representantes eleitos.

Serviços de consultoria e assessoria, inclusive dar conselhos ou prestar serviços profissionais, e a prestação de serviços de assessoria, consultoria ou natureza intermediária.

Referência de crédito, incluindo o fornecimento de informações por agências de referência de crédito relacionadas à situação financeira de indivíduos ou organizações em nome de outras organizações

Análise de dados, incluindo criação de perfis

Administração de dívidas e factoring, inclusive a localização de devedores comerciais e de consumidores e a cobrança em nome de credores, e a compra de dívidas comerciais ou de consumidores de empresas, inclusive aluguéis e pagamentos de crédito parcelado.

Educação, incluindo o fornecimento de educação ou treinamento como função principal ou como atividade comercial.

Serviços financeiros e consultoria, incluindo a prestação de serviços como intermediário em relação a quaisquer transações financeiras, incluindo hipotecas e corretagem de seguros

Arrecadação de fundos em apoio aos objetivos do exportador de dados

Administração e serviços de saúde, incluindo o fornecimento e a administração de cuidados com o paciente.

Administração de informações e bancos de dados, incluindo a manutenção de informações ou bancos de dados como ferramenta de referência ou recurso geral. Isso inclui catálogos, listas, diretórios e bancos de dados bibliográficos.

Administração de seguros, incluindo a administração de seguros de vida, saúde, pensões, propriedade, automóvel e outros negócios de seguros por uma empresa de seguros, um intermediário ou consultor de seguros

Serviços de TI, digitais, de tecnologia ou de telecomunicações, incluindo o uso de produtos ou serviços de tecnologia, serviços de telecomunicações e de rede, serviços digitais, hospedagem, nuvem e serviços de suporte ou software

Jornalismo e mídia, incluindo o processamento de material jornalístico, literário ou artístico feito ou destinado a ser disponibilizado ao público ou a qualquer seção do público.

Serviços jurídicos, inclusive assessoria e atuação em nome de clientes.

Licenciamento e registro, incluindo a administração de licenciamento ou manutenção de registros oficiais.

Atividades de organizações sem fins lucrativos, incluindo

- estabelecer ou manter a filiação ou o apoio a um órgão ou associação sem fins lucrativos, e

- fornecer ou administrar atividades para indivíduos que sejam membros da entidade ou associação sem fins lucrativos ou que tenham contato regular com ela.

Cuidado pastoral, incluindo a administração do cuidado pastoral por um vigário ou outro ministro da religião.

Administração de pensões, inclusive a administração de pensões financiadas ou planos de aposentadoria.

Compras, incluindo a decisão de aceitar qualquer pessoa ou organização como fornecedor e a administração de contratos, medidas de desempenho e outros registros.

Investigação particular, incluindo a prestação, em bases comerciais, de serviços de investigação de acordo com as instruções dadas pelos clientes

Gerenciamento de propriedades, incluindo o gerenciamento e a administração de terrenos, propriedades e imóveis residenciais, e o gerenciamento de patrimônio de outras organizações.

Realização dos objetivos de uma organização beneficente ou entidade voluntária, incluindo o fornecimento de bens e serviços para a realização dos objetivos da organização beneficente ou entidade voluntária.

Pesquisa em qualquer campo, inclusive pesquisa de mercado, saúde, estilo de vida, científica ou técnica.

Segurança de pessoas e propriedades, incluindo o uso de sistemas de CCTV para essa finalidade.

Comércio/compartilhamento de informações pessoais, incluindo a venda, aluguel, troca ou divulgação de informações pessoais a

terceiros em troca de bens/serviços/benefícios.

Outras atividades (forneça detalhes):

Importador de dados

O importador de dados é uma empresa de tecnologia sediada em Cingapura que fornece ao exportador de dados uma plataforma de gerenciamento de crescimento para suas atividades de marketing multicanal.

Sujeitos de dados

O Exportador de Dados pode enviar Dados Pessoais ao Importador de Dados e suas Afiliadas, cuja extensão é determinada e controlada pelo Exportador de Dados a seu exclusivo critério, e que pode incluir, mas não se limita a Dados Pessoais relacionados às seguintes categorias de titulares de dados:

-Clientes em potencial, clientes, revendedores, referenciadores, parceiros comerciais e fornecedores do exportador de dados (que são pessoas físicas);

-Funcionários ou pessoas de contato de clientes em potencial, clientes, revendedores, consultores, subcontratados, parceiros comerciais e fornecedores do exportador de dados (que sejam pessoas físicas);

-Funcionários, agentes, consultores e freelancers do exportador de dados (que são pessoas físicas); e/ou

-Pessoas físicas autorizadas pelo exportador de dados a usar os serviços fornecidos pelo importador de dados ao exportador de dados.

Categorias de dados

Os dados pessoais transferidos referem-se às seguintes categorias de dados:

O Exportador de Dados pode enviar Dados Pessoais ao Importador de Dados e suas Afiliadas, cuja extensão é determinada e controlada pelo Exportador de Dados a seu exclusivo critério, e que pode incluir, mas não se limita às seguintes categorias de Dados Pessoais:

Detalhes pessoais, inclusive qualquer informação que identifique o titular dos dados e suas características pessoais, incluindo: nome, endereço, detalhes de contato, idade, data de nascimento, sexo e descrição física.

Família, estilo de vida e circunstâncias sociais, inclusive quaisquer informações relacionadas à família do titular dos dados e ao estilo de vida e circunstâncias sociais do titular dos dados, inclusive casamento e parcerias atuais, histórico conjugal, detalhes da família e de outros membros da casa, hábitos, moradia, detalhes de viagens, atividades de lazer e participação em organizações beneficentes ou voluntárias.

Detalhes de educação e treinamento, inclusive informações relacionadas à educação e a qualquer treinamento profissional do titular dos dados, incluindo registros acadêmicos, qualificações, habilidades, registros de treinamento, experiência profissional, registros de alunos e de estudantes.

Detalhes de emprego, inclusive informações relacionadas ao emprego do titular dos dados, incluindo histórico de emprego e carreira, detalhes de recrutamento e rescisão, registros de presença, registros de saúde e segurança, avaliações de desempenho, registros de treinamento e registros de segurança.

Detalhes financeiros, inclusive informações relacionadas aos assuntos financeiros do titular dos dados, incluindo renda, salário, ativos e investimentos, pagamentos, capacidade de crédito, empréstimos, benefícios, subsídios, detalhes de seguros e informações sobre pensões.

Bens ou serviços fornecidos e informações relacionadas, incluindo detalhes dos bens ou serviços fornecidos, licenças emitidas e contratos.

Dados pessoais relacionados a condenações e ofensas criminais

Outros (forneça detalhes de outros titulares de dados):

Operações de processamento

Os dados pessoais transferidos estarão sujeitos às seguintes atividades básicas de processamento definidas neste adendo.

Recebimento de dados, incluindo coleta, acesso, recuperação, registro e entrada de dados

Manutenção de dados, incluindo armazenamento, organização e estruturação

Uso de dados, incluindo análise, consulta, teste, tomada de decisão automatizada e criação de perfil

Atualização de dados, incluindo correção, adaptação, alteração, alinhamento e combinação

Proteção de dados, incluindo restrição, criptografia e testes de segurança

Devolução de dados ao exportador de dados ou ao titular dos dados

Apagamento de dados, incluindo destruição e exclusão

Apêndice 2

Medidas de segurança

- A. O importador/subprocessador de dados implementou e deve manter um programa de segurança de acordo com os padrões do setor.
B. Mais especificamente, o programa de segurança do importador/subprocessador de dados deverá incluir:

Acesso às operações internas do importador de dados

O importador/subprocessador de dados implementa medidas ideais para evitar que pessoas não autorizadas tenham acesso ao equipamento de processamento de dados onde os dados pessoais são processados ou usados, inclusive:

- estabelecer áreas de segurança;
- proteção e restrição de caminhos de acesso;
- estabelecer autorizações de acesso para funcionários e terceiros, incluindo a respectiva documentação;
- todo o acesso ao centro de dados onde os dados pessoais estão hospedados é registrado, monitorado e rastreado; e
- O data center onde os dados pessoais são hospedados é protegido por um sistema de alarme de segurança e outras medidas de segurança apropriadas.

Acesso ao sistema

O importador de dados implementa medidas ideais para evitar que seus sistemas de processamento de dados sejam usados por pessoas não autorizadas, inclusive:

- uso de tecnologias de criptografia adequadas;
- identificação do terminal e/ou do usuário do terminal para o importador de dados/subprocessador e sistemas de processamento;
- bloqueio temporário automático da ID do usuário quando várias senhas erradas são inseridas e
- todo acesso ao conteúdo de dados é registrado, monitorado e rastreado.

Acesso ao uso de áreas específicas de processamento de dados

O importador/subprocessador de dados compromete-se a garantir que as pessoas autorizadas a usar seu sistema de processamento de dados só possam acessar os dados dentro do escopo e na extensão cobertos por sua respectiva permissão de acesso (autorização) e que os dados pessoais não possam ser lidos, copiados, modificados ou removidos sem autorização. Isso deve ser feito por meio de várias medidas, incluindo:

- políticas e treinamento de funcionários com relação aos direitos de acesso de cada funcionário aos dados pessoais;
- alocação de terminais individuais e/ou usuário do terminal e características de identificação exclusivas para funções específicas;
- capacidade de monitoramento em relação aos indivíduos que excluem, adicionam ou modificam os dados pessoais;
- liberação de dados somente para pessoas autorizadas, incluindo a alocação de direitos e funções de acesso diferenciados;
- uso de tecnologias de criptografia adequadas; e controle de arquivos, destruição controlada e documentada de dados.

Transporte

O importador/subprocessador de dados implementa medidas adequadas para evitar que os dados pessoais sejam lidos, copiados, alterados ou excluídos por partes não autorizadas durante a transmissão ou durante o transporte da mídia de dados. Isso é realizado por várias medidas, incluindo:

- uso de tecnologias adequadas de firewall, VPN e criptografia para proteger os gateways e pipelines pelos quais os dados trafegam;
- determinados dados altamente confidenciais dos funcionários (por exemplo, informações de identificação pessoal, como números de identidade nacional, números de cartões de crédito ou débito) também são criptografados no sistema; e
- fornecer alerta ao usuário em caso de transferência incompleta de dados (verificação de ponta a ponta); e, na medida do possível, todas as transmissões de dados são registradas, monitoradas e rastreadas.

Entrada

O importador/subprocessador de dados implementa medidas adequadas de controle de entrada, inclusive:

- uma política de autorização para a entrada, leitura, alteração e exclusão de dados;

- autenticação do pessoal autorizado;
- medidas de proteção para a entrada de dados na memória, bem como para a leitura, alteração e exclusão de dados armazenados;
- utilização de credenciais ou códigos de autenticação exclusivos (senhas);
- log-off automático de IDs de usuário que não tenham sido usadas por um período substancial de tempo; e
- prova estabelecida dentro da organização do importador de dados/subprocessador da autorização de entrada; e
- registro eletrônico de entradas.

Documentação

O importador/subprocessador de dados manterá a documentação das medidas técnicas e organizacionais em caso de auditorias e para a conservação de evidências. O Importador/subprocessador de dados deverá tomar medidas razoáveis para garantir que as pessoas empregadas por ele e outras pessoas no local de trabalho em questão estejam cientes e cumpram as medidas técnicas e organizacionais estabelecidas neste DPA.

Controle

O importador/subprocessador de dados deverá implementar medidas ideais para monitorar as restrições de acesso aos administradores de sistema do importador/subprocessador de dados e para garantir que eles ajam de acordo com as instruções recebidas. Isso é feito por meio de várias medidas, incluindo:

- nomeação individual de administradores de sistema;
- adoção de medidas ideais para registrar os logs de acesso dos administradores de sistemas à infraestrutura e mantê-los seguros, precisos e inalterados por pelo menos seis meses;
- auditorias anuais das atividades dos administradores de sistemas para avaliar a conformidade com as tarefas atribuídas, as instruções recebidas pelo importador/subprocessador de dados e as leis aplicáveis;
- manter uma lista atualizada com os detalhes de identificação dos administradores do sistema (por exemplo, nome, sobrenome, função ou área organizacional) e as tarefas atribuídas e fornecê-la prontamente ao exportador de dados mediante solicitação.

Em nome do exportador de dados:

Nome (escrito por extenso):

Posição:

Endereço:

Outras informações necessárias para que o contrato seja vinculativo (se houver):

Assinatura:

Em nome do importador de dados:

Nome (escrito por extenso):

Posição:

Endereço:

Outras informações necessárias para que o contrato seja vinculativo (se houver):

Assinatura: