CONTRATO DE PROTEÇÃO DE DADOS (DPA)

O Cliente deverá disponibilizar à SINCH e o Cliente autoriza a SINCH a tratar informações, incluindo dados pessoais para a prestação dos Serviços nos termos do Contrato (doravante denominado "Contrato"). As partes concordaram em celebrar este Contrato de Proteção de Dados, doravante denominado simplesmente como “DPA”, para confirmar as regras de proteção de dados relativas ao seu relacionamento, bem como para cumprir os requisitos da Legislação de Proteção de Dados aplicável.

1. DEFINIÇÕES

1.1 Para os fins deste DPA:

"**Legislação de Proteção de Dados**" significa a legislação que protege os direitos e liberdades fundamentais dos indivíduos e, em particular, o seu direito à privacidade no que diz respeito ao tratamento de dados pessoais pelo Cliente como controlador de dados, incluindo, sem limitação, todas as leis (inter)nacionais vinculativas e outras diretivas vinculativas de proteção de dados ou segurança de dados, leis, regulamentos e decisões válidas em determinado momento, incluindo quaisquer orientações e códigos de práticas emitidos pela autoridade supervisora aplicável;

"**Dados Pessoais**" significa qualquer informação relativa a uma pessoa física identificada ou identificável ("**titular dos dados**"); uma pessoa identificável é aquela que poderá ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização, identificador online ou a um ou mais fatores específicos de ordem física, fisiológica, genética, identidade mental, econômica, cultural ou social dessa pessoa;

"**Tratamento de (Dados)**" significa qualquer operação ou conjunto de operações realizadas sobre Dados Pessoais ou conjuntos de Dados Pessoais, seja ou não por meios automatizados, tais como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, extração, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, eliminação ou destruição;

"**Dados pessoais sensíveis**" significa informações sobre origem racial ou étnica, opiniões políticas, convicção religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde, dados relativos à vida sexual ou orientação sexual de uma pessoa física ou qualquer outro categoria especial de dados conforme indicado no Anexo 2 Alterações específicas *com base na legislação nacional aplicável* ou na Ordem de Serviço ou Especificação de Serviço;

"**Medidas Técnicas e Organizacionais**" ou TOMs significa medidas destinadas a proteger Dados Pessoais contra destruição acidental ou ilícita ou perda acidental, alteração, divulgação ou acesso não autorizado. Isso inclui os requisitos de segurança aplicáveis acordados, as instruções de segurança e suas atualizações aplicáveis a cada momento, descritas no Anexo 1 *Medidas Técnicas e Organizacionais* deste DPA ou na Ordem de Serviço ou Especificação do Serviço;

Os termos "**controlador de dados**" e "**operador de dados**" terão os significados que lhes são atribuídos na GDPR.

1.2 Termos em letras maiúsculas utilizados e não definidos neste DPA têm os significados atribuídos no Contrato.

2. RESPONSABILIDADE DAS PARTES

As partes entendem que para a prestação dos Serviços é feita uma distinção entre dois tipos de tratamento de Dados Pessoais: (i) a prestação dos serviços (ou seja, o banco de dados de registros de dados de chamadas e os logs criados e gerenciados pela SINCH em nome e sob a supervisão do Cliente) para o qual a SINCH atuará como um operador de dados e concorda em cumprir com as respectivas obrigações estabelecidas neste DPA, e (ii) a transmissão de mensagens (ex. A2P, SMS) pela Sinch e outros Provedores de Serviços para os quais a SINCH atuará como controlador de dados e

3. OBJETO, NATUREZA E FINALIDADE DO TRATAMENTO DE DADOS PESSOAIS DA SINCH

3.1 O objeto, a natureza e a finalidade do tratamento de Dados Pessoais nos termos deste DPA são a execução dos Serviços por parte da SINCH nos termos do Contrato e conforme instruído posteriormente

pelo Cliente em seu uso dos Serviços ("**Instruções**"), a menos que seja necessário fazê-lo de forma diversa conforme estabelecido e na medida permitida pela Legislação de Proteção de Dados e/ou Leis Relevantes.

3.2 As instruções do Cliente deverão ser por escrito (incluindo, mas não se limitando a, e-mail) ou poderão ser fornecidas por meio de configurações e uso do(s) portal(ais) e/ou software da SINCH. Em casos excepcionais, as Instruções poderão ser fornecidas oralmente pelo Cliente. Essas Instruções orais serão confirmadas pela pessoa autorizada do Cliente por escrito ou por e-mail (em formato de texto).

4. DURAÇÃO

4.1 A SINCH deverá apenas coletar ou tratar Dados Pessoais durante a vigência do Contrato na medida e conforme necessário para a prestação dos Serviços e de acordo com o Contrato e a Legislação de Proteção de Dados aplicável à SINCH conforme sua função no tratamento de Dados Pessoais.

4.2 O tratamento de Dados Pessoais será realizado pela SINCH após o término do Contrato desde que necessário para cumprir com as obrigações deste DPA ou quando necessário devido à obrigação legal, salvo acordo expresso das partes de forma diversa.

5. TIPO DE DADOS PESSOAIS TRATADOS

As seguintes categorias de Dados Pessoais poderão ser tratatadas para fornecer os Serviços, cuja extensão é determinada e controlada pelo Cliente a seu exclusivo critério e poderá incluir, mas não está limitada às seguintes categorias de Dados Pessoais:

- Informações de contato (empresa, e-mail, telefone, endereço físico)
- Primeiro e último nome
- Dados de identificação
- Cargo
- Função
- Empregador
- Dados de conexão
- Dados de localização
- Outros dados, conforme definido no Contrato, conforme acordado entre as partes.

6. TIPO DE TITULARES DE DADOS

O Cliente poderá enviar Dados Pessoais através da utilização dos Serviços, cuja extensão é determinada e controlada pelo Cliente a seu exclusivo critério, e que poderão incluir, mas não estão limitados a Dados Pessoais relacionados às seguintes categorias de titulares de dados:

- Clientes, parceiros de negócios e fornecedores do Cliente (que são pessoas físicas)
- Funcionários de pessoas de contato dos clientes, parceiros de negócios e fornecedores do Cliente
- Funcionários, agentes, consultores, autônomos do Cliente (que sejam pessoas físicas)
- Usuário dos Serviços do Cliente, incluindo qualquer usuário dos Serviços, que o Cliente permita usar os Serviços

7. SUBOPERADORES

7.1 O Cliente concorda que a SINCH poderá envolver uma Afiliada da Sinch ou terceiros para tratar dados pessoais a fim de ajudar a SINCH a fornecer os Serviços em nome do Cliente ("**Suboperadores**"). A SINCH tem ou irá celebrar um acordo por escrito com cada Suboperador contendo obrigações de proteção de dados que não sejam menos estritas do que aquelas que constam deste DPA, na medida aplicável à natureza dos Serviços fornecidos por tal Suboperador.

7.2 Quando exigido por lei, a SINCH deverá concluir acordos adicionais (por exemplo, entre outros, Contratos de Associados Comerciais, conforme exigido pela Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 ("HIPAA") e/ou Tecnologia da Informação em Saúde para Economia e Lei de Saúde Clínica ("HITECH").

7.3 Os atuais Suboperadores dos Serviços são definidos em https://www.sinch.com/data-protection-agreement/sub-processors/ ("**Lista de Suboperadores**") e o Cliente concorda e aprova os Suboperadores para que tratem os Dados Pessoais O Cliente poderá encontrar em https://www.sinch.com/data-protection-agreement/sub-processors/ um mecanismo através do qual

receba notificações relativas a novos Suboperadores para cada Serviço aplicável e desde que subinscrito, a SINCH fornecerá notificação do(s) novo(s) Suboperador(es) antes de autorizar qualquer(s) novo(s) Suboperador(es) a tratar Dados Pessoais em conexão com o fornecimento do Serviço aplicável.

7.4 A SINCH deverá notificar o Cliente com 30 dias de antecedência, conforme estabelecido na cláusula 10.2, , sobre quaisquer alterações pretendidas relativas à adição ou substituição de qualquer Suboperador durante o qual o Cliente poderá fazer objeções à nomeação do Suboperador. Quaisquer objeções deverão ser feitas imediatamente (e em qualquer caso, no máximo catorze (14) dias após a notificação da SINCH das alterações pretendidas). Caso a SINCH opte por manter o Suboperador da objeção, a SINCH notificará o Cliente com pelo menos quatorze (14) dias antes de autorizar o Suboperador a tratar dados pessoais e, em seguida, o Cliente poderá interromper imediatamente o uso da parte relevante dos Serviços e poderá encerrar a parte relevante dos Serviços. Caso aplicável, a SINCH reembolsará o Cliente por quaisquer taxas pré-pagas cobrindo o restante do prazo de tal parte relevante do Serviço após a data efetiva de rescisão, não havendo penalidade para nenhuma das partes.

7.5 A SINCH poderá substituir um Suboperador sem aviso prévio quando o motivo da alteração estiver fora do controle razoável da SINCH e a substituição imediata se fizer necessária por motivos de segurança ou outros motivos urgentes, incluindo mas sem se limitar a não conformidade de um Suboperador com a Legislação de Proteção de Dados ou DPA entre SINCH e o Suboperador. Neste caso, a SINCH informará o controlador de Dados sobre a substituição do Suboperador assim que possível após sua nomeação. A Seção 7.4 se aplica, por conseguinte.

7.6 Para evitar dúvidas, quando qualquer Suboperador deixar de cumprir suas obrigações sob qualquer contrato de subtratamento ou sob a lei aplicável, a SINCH permanecerá totalmente responsável perante o Cliente pelo cumprimento de suas obrigações nos termos deste DPA.

8. TRANSFERÊNCIA INTERNACIONAL

8.1 Sempre que a SINCH (ou seus Suboperadores) tratar Dados Pessoais em outros países que não o país em que a SINCH está estabelecida, a SINCH garantirá um nível adequado de proteção de Dados Pessoais por meio de medidas organizacionais, técnicas e contratuais conforme exigido pela Legislação de Proteção de Dados aplicável e este DPA.

8.2 Quando (i) Dados Pessoais de outro controlador de Dados são tratados internacionalmente e tal tratamento internacional requeira um meio de adequação de acordo com as leis do país do controlador de Dados, incluindo mas não limitado à adequação e ao cumprimento das Cláusulas Contratuais Padrão Europeias aprovadas pela Comissão Europeia para a transferência de dados pessoais. O Cliente fornece uma procuração para que a SINCH possa celebrar quaisquer Cláusulas Contratuais Padrão Europeias aprovadas pela Comissão Europeia com um Suboperador aprovado conforme estabelecido na cláusula 7 em nome do Cliente, ou quando (ii) os Dados Pessoais de um controlador de Dados baseado no Espaço Econômico Europeu (EEE) ou na Suíça são tratados em um país fora do EEE, Suíça e qualquer país, organização ou território reconhecido pela União Europeia como país seguro com um nível adequado de proteção de dados nos termos do art. 45 GDPR e nenhum outro mecanismo de transferência legal, como Regras Corporativas Vinculativas (art. 47 GDPR) ou Código de Conduta (art. 40 GDPR).

8.3 No caso de a Comissão Europeia aprovar Cláusulas Contratuais Padrão Europeias celebradas entre a SINCH e o Cliente, respectivas cláusulas se aplicam até que uma autoridade supervisora competente de um Estado-Membro, ou de um tribunal da União Europeia ou de um Estado-Membro competente aprove um novo mecanismo de transferência legal aplicável às transferências de dados cobertas pelas Cláusulas Contratuais Padrão Europeias (no caso de tal mecanismo se aplicar apenas a algumas das transferências de dados, as Cláusulas Contratuais Padrão Europeias permanecerão aplicáveis para as transferências que não poderão ser cobertas pelo novo mecanismo de transferência legal):

(i) Os direitos concedidos aos titulares dos dados ao abrigo deste DPA e das Cláusulas Contratuais Padrão Europeias poderão ser aplicados pelo titular dos dados contra a SINCH, independentemente de qualquer restrição nas Cláusulas 3 ou 6 das Cláusulas Contratuais Padrão Europeias. Respectivos direitos são pessoais e não poderão ser atribuídos a terceiros. O titular dos dados só poderá apresentar uma reclamação ao abrigo deste DPA e das Cláusulas Contratuais Padrão Europeias individualmente, e não como parte de uma ação coletiva, de grupo ou representativa.

(ii) Além da Cláusula 5 (b) das Cláusulas Contratuais Padrão Europeias, a SINCH concorda que, no momento da celebração deste Contrato, não tem motivos para acreditar que a legislação aplicável a SINCH ou a seus Suboperador, incluindo em qualquer país em que os Dados Pessoais são transferidos pela SINCH ou por meio de um Suboperador, a impede de cumprir as instruções recebidas do Cliente e suas obrigações nos termos das Cláusulas Contratuais Padrão Europeias e que, no caso de uma alteração nesta legislação, que provavelmente terá um efeito adverso nas garantias e obrigações

previstas nas Cláusulas Contratuais Padrão Europeias, notificará a alteração ao Cliente assim que tiver conhecimento, caso em que o Cliente tem o direito de suspender a transferência de dados e/ou rescindir o Contrato.

(iii) Para os fins desta seção, os esforços legais não incluem ações que resultariam em penalidades civis ou criminais, como desacato ao tribunal sob as leis da jurisdição relevante:

- Caso a SINCH receba um pedido de terceiros para divulgação forçada de quaisquer Dados Pessoais que tenham sido transferidos de acordo com as Cláusulas Contratuais Padrão Europeias, a SINCH deverá, sempre que possível, redirecionar o terceiro para solicitar dados diretamente do Cliente.

- Caso a SINCH receba um pedido de qualquer terceiro para a divulgação forçada de quaisquer Dados Pessoais que tenham sido transferidos de acordo com as Cláusulas Contratuais Padrão Europeias, a SINCH envidará todos os esforços legais para contestar o pedido de divulgação com base em quaisquer deficiências legais sob as leis da parte requerente ou quaisquer conflitos relevantes com a legislação da União Europeia ou com a legislação aplicável dos Estados-Membros.

9. MEDIDAS TÉCNICAS E ORGANIZACIONAIS

A SINCH implementou e mantém medidas técnicas e organizacionais adequadas para proteger Dados Pessoais tratados contra tratamentos não autorizado ou ilegal e contra perda acidental, destruição, dano, alteração ou divulgação. Estas medidas são descritas no Anexo 1 *Medidas Técnicas e Organizacionais*.

10. GARANTIAS DE QUALIDADE E OUTRAS FUNÇÕES DA SINCH

10.1 A SINCH deverá cumprir os seguintes requisitos, sendo:

- não realizar nenhum tratamento de Dados Pessoais, exceto por instruções do controlador de Dados e/ou quando exigido por uma autoridade nos termos da lei;
- implementar um registro de tratamento de dados
- implementar medidas técnicas e organizacionais para garantir um nível de segurança de dados adequado ao nível de risco apresentado pelo tratamento de Dados Pessoais;
- cooperar com a autoridade supervisora de proteção de dados no desempenho de suas funções
- notificar a violação de Dados Pessoais à autoridade supervisora e ao titular dos dados;
- realizar uma avaliação de impacto à proteção de dados quando necessário de acordo com a lei e consultar a autoridade supervisora antes do tratamento de dados, quando a avaliação de impacto à proteção de dados indicar que o tratamento resultaria em um alto risco na ausência de medidas tomadas pelo controlador de Dados para mitigar o risco.

e garante, em particular, o cumprimento dos seguintes requisitos:

a) Nomear um encarregado pelo tratamento de dados pessoais, que desempenhará suas funções em conformidade com a Legislação de Proteção de Dados. Os detalhes de contato do encarregado ~~oficial~~ de proteção de dados (DPO) estão disponíveis na página oficial da SINCH na web. Caso a parte contratante da SINCH não estiver estabelecida na União Europeia, a SINCH nomeará uma pessoa de contato responsável na União Europeia e/ou um encarregado ~~oficial~~ de proteção de dados de acordo com a Legislação de Proteção de Dados.

b) Confidencialidade de acordo com a Legislação de Proteção de Dados. A SINCH confia o tratamento de dados descrito neste Contrato apenas aos funcionários que estão sujeitos à confidencialidade e que foram previamente familiarizados com as disposições de proteção de dados relevantes para seu trabalho. A SINCH e qualquer pessoa agindo sob sua autoridade que tenha acesso aos Dados Pessoais, não deverá tratar esses dados, a menos que sob instruções do Cliente (o que inclui os poderes concedidos neste DPA), e/ou, a menos que exigido pela Legislação de Proteção de Dados.

c) Às custas e despesas do Cliente e levando em consideração a natureza do tratamento e as informações disponíveis para a SINCH, fornecer as informações e assistência que o Cliente possa razoavelmente exigir e dentro dos prazos razoavelmente especificados pelo Cliente para auxiliar o Cliente a cumprir suas obrigações sob a Legislação de Proteção de Dados aplicável, que poderá incluir ajudar o Cliente a:

   i) notificar o Cliente de qualquer solicitação que a SINCH receba para um titular de dados relativos a dados pessoais tratados e notificar o titular dos dados para entrar em contato com o Cliente se quiser usar seus direitos;
   ii) cumprir suas obrigações de segurança;
   iii) cumprir suas obrigações de responder às solicitações relacionadas ao exercício dos direitos do titular dos dados, incluindo direito de acesso, direito de retificação, direito de apagamento ("direito

de ser esquecido") direito de restrição de tratamento (na medida em que os dados pessoais não estejam acessíveis ao Cliente por meio dos Serviços); realizar a Avaliação do Impacto à Proteção de Dados e auditar a conformidade da Avaliação do Impacto à Proteção de Dados e consultar a autoridade supervisora;

iv) seguir a Avaliação de Impacto à Proteção de Dados.

d) Para os fins desta seção, os esforços legais não incluem ações que resultariam em penalidades civis ou criminais, como desacato ao tribunal sob as leis da jurisdição relevante:

i) A menos que proibido pela lei aplicável ou por um pedido legalmente vinculativo de aplicação da lei, a SINCH notificará imediatamente o Cliente de qualquer pedido por, qualquer funcionário do governo, autoridade supervisora de proteção de dados ou autoridade policial em relação a quaisquer dados pessoais e, se proibido de notificar o Cliente, a SINCH envidará todos os esforços legais para obter o direito de renunciar à proibição a fim de comunicar o máximo de informações ao Cliente o mais rápido possível;

e) A SINCH deverá monitorar periodicamente os processos internos e os TOMs para garantir que o tratamento dentro da área de responsabilidade da SINCH esteja de acordo com os requisitos da Legislação de Proteção de Dados e a proteção dos direitos do titular dos dados.

11. AUDITORIAS E INSPEÇÕES

11.1 No caso de o Cliente, um Regulador ou autoridade de proteção de dados exigir informações adicionais ou uma auditoria relacionada aos Serviços, então, a SINCH concorda em conceder acesso às suas instalações de tratamento de dados, arquivos de dados e documentação necessária para o tratamento de Dados Pessoais. A SINCH concorda em fornecer cooperação razoável durante tais operações, incluindo o fornecimento de todas as informações relevantes e acesso a todos os equipamentos, software, dados, arquivos, sistemas de informação etc., usados para a execução dos Serviços, incluindo o tratamento de Dados Pessoais.

11.2 O direito de auditoria, conforme descrito na cláusula 11.1, será aplicável para o Cliente, caso a SINCH não tenha fornecido evidências suficientes de seu cumprimento das medidas técnicas e organizacionais. Evidências suficientes incluem o fornecimento de: (i) uma certificação quanto à conformidade com a ISO 27001 ou outras normas implementadas pela SINCH (escopo conforme definido no certificado); ou (ii) um relatório de auditoria ou certificação de um terceiro independente. Uma auditoria conforme descrito na cláusula 11.1 deverá ser realizada por conta e custo do Cliente. Uma auditoria poderá ser feita pelo Cliente ou qualquer terceiro razoavelmente aceitável para a SINCH (que não deverá incluir quaisquer auditores terceiros que sejam concorrentes da SINCH ou não devidamente qualificados ou independentes) para verificar a conformidade com este DPA, bem como o cumprimento das medidas técnicas e organizacionais da SINCH, desde que mediante aviso prévio razoável de no mínimo trinta (30) dias e celebração de um acordo de não divulgação diretamente entre SINCH e o auditor.

12. NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS

12.1 Caso a SINCH fique ciente de qualquer violação de segurança que resulte na destruição acidental, não autorizada ou ilícita ou na divulgação não autorizada ou no acesso a Dados Pessoais, a SINCH deverá, entre outras coisas:

a) Notificar o Cliente por escrito imediatamente, mas não depois de 72 horas após tomar conhecimento da violação de Dados Pessoais;

b) Auxiliar o Cliente no que diz respeito à obrigação do Cliente de fornecer informações ao titular dos dados e de fornecer ao Cliente informações relevantes a esse respeito;

c) Apoiar o Cliente em consultas com autoridade de proteção de dados.

12.2 Na medida do legalmente possível, a SINCH poderá reclamar uma compensação pelos serviços de apoio nos termos desta cláusula 12 que não sejam atribuíveis a violações de Dados Pessoais causadas pela SINCH.

13. ELIMINAÇÃO DE DADOS PESSOAIS

13.1 A SINCH é obrigada a apagar os Dados Pessoais conforme estipulado no Contrato e de acordo com a Legislação de Proteção de Dados e/ou Leis Relevantes.

13.2 O Cliente tem o direito de solicitar a execução dos direitos e obrigações descritos na cláusula 13.1 durante a duração de todo o DPA.

13.3 As obrigações legais de retenção ou obrigações contratuais para com os Prestadores de Serviços da SINCH (por exemplo, mas não limitado aos operadores) permanecem inalteradas pelas disposições acima. A documentação que serve como evidência para um tratamento de dados ordenado de acordo com as disposições do DPA deverá ser retida pela SINCH após o encerramento do DPA de acordo com a Legislação de Proteção de Dados e/ou Leis Relevantes.

14. OBRIGAÇÕES DA SINCH COMO CONTROLADOR DE DADOS

Em situações em que a SINCH atuará como controlador de Dados, ela se compromete a cumprir com suas obrigações nos termos da Legislação de Proteção de Dados aplicável em relação a quaisquer dados pessoais tratados em relação ao Contrato e aos Serviços. A SINCH deverá tratar esses dados pessoais em conexão com a transmissão de mensagens e para cumprir suas obrigações associadas nos termos do Contrato ou conforme exigido por lei, ordem judicial ou qualquer autoridade governamental ou reguladora e de acordo com sua política de privacidade, que está disponível em https://www.sinch.com/privacy-policy/ conforme alterado de tempos em tempos, se necessário.

15. OBRIGAÇÕES DO CLIENTE

O Cliente deverá cumprir em todos os momentos a Legislação de Proteção de Dados em relação ao tratamento de dados pessoais em conexão com o Contrato e os Serviços. O Cliente deverá informar a SINCH por escrito caso seja aplicável legislação adicional ao Tratamento de Dados Pessoais que não a legislação do país onde o Cliente está estabelecido.

16. LIMITAÇÃO DE RESPONSABILIDADE

16.1 A responsabilidade de cada parte e de todas as suas Afiliadas, em conjunto no agregado, decorrente de ou relacionada a este DPA seja em contrato, ato ilícito ou sob qualquer outra teoria de responsabilidade, está sujeita à seção de Limitação de Responsabilidade do Contrato, e qualquer referência em tal seção à responsabilidade de uma parte significa a responsabilidade agregada dessa parte e de todas as suas Afiliadas nos termos do Contrato e deste DPA.

16.2 A cláusula 16.1 não se aplica se o dano tiver sido causado pela implementação incorreta do serviço encomendado realizada pelo Cliente ou por uma instrução dada pelo Cliente. Nesse caso, o Cliente será responsável por tais danos.

17. DISPOSIÇÕES DIVERSAS

17.1 O DPA é parte integrante do Contrato entre o Cliente e a SINCH. Em caso de conflito entre as disposições obrigatórias nas Cláusulas Contratuais Padrão Europeias e este DPA, as Cláusulas Contratuais Padrão Europeias prevalecem. Em caso de outros conflitos entre outros documentos (inclusive em caso de conflito entre o Contrato e este DPA), o DPA prevalecerá.

17.2 Caso qualquer disposição deste DPA seja ou se torne inválida ou contenha uma lacuna, as disposições restantes não serão afetadas. O Cliente e a SINCH comprometem-se a substituir a disposição inválida por disposições legalmente válidas que mais se aproximam do interesse da disposição inválida, respectivamente, que preenche a lacuna.

ANEXO 1 ao Contrato de Proteção de Dados – Medidas Técnicas e Organizacionais

A SINCH implementará as medidas descritas neste Anexo 1, desde que as medidas contribuam direta ou indiretamente ou possam contribuir para a proteção de Dados Pessoais no âmbito do Contrato celebrado entre as partes para o tratamento de dados.

As medidas técnicas e organizacionais que são implementadas pela SINCH são baseadas no estado atual da tecnologia, os custos de implementação e a natureza, âmbito, circunstâncias e finalidades do tratamento e a probabilidade e gravidade do risco aos direitos e liberdades dos indivíduos são verdadeiras. As Medidas Técnicas e Organizacionais estão sujeitas ao progresso e desenvolvimento técnico. A este respeito, a SINCH está autorizada a implementar medidas alternativas adequadas. O nível de segurança deverá estar alinhado com as melhores práticas de segurança do setor e não menos do que as medidas aqui estabelecidas. Todas as principais alterações deverão ser acordadas com o Cliente e documentadas.

As Medidas Técnicas e Organizacionais incluídas neste Anexo 1 são medidas aplicáveis ao(s) Serviço(s) prestado(s) pela SINCH. Se necessário, para o Serviço, a SINCH poderá incluir outras medidas técnicas e organizacionais na Ordem de Serviço ou Especificação de Serviço.

1 Gestão de riscos e Procedimentos para validação, revisão e avaliação

i. A SINCH deverá identificar e avaliar os riscos de segurança relacionados à confidencialidade, integridade e disponibilidade e, com base nessa avaliação, implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco.

ii. A SINCH deverá ter processos e rotinas documentados para lidar com os riscos em suas operações e ao tratar dados pessoais em nome do Cliente.

iii. A SINCH deverá avaliar periodicamente os riscos relacionados aos sistemas de informação e tratamento, armazenamento e transmissão de informações.

iv. A SINCH deverá identificar e avaliar os riscos de segurança relacionados à confidencialidade, integridade e disponibilidade e, com base em tal avaliação, implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco dos tipos e finalidades de Dados Pessoais específicos sendo tratados pela SINCH, incluindo, entre outros, conforme o caso:

   a) A pseudonimização e criptografia de dados pessoais;
   b) A capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de tratamento;
   c) A capacidade de restaurar a disponibilidade e o acesso aos Dados do Cliente em tempo hábil no caso de um incidente físico ou técnico;

v. Um processo para testar regularmente, avaliar e avaliar a eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento.

vi. A SINCH deverá avaliar periodicamente os riscos relacionados aos sistemas de informação e tratamento de dados pessoais (por exemplo, ao armazenar e transmitir dados pessoais).

vii. A Sinch deverá monitorar, revisar e auditar regularmente a conformidade do Suboperador com as Medidas Técnicas e Organizacionais e a Sinch deverá, a pedido do Cliente, fornecer ao Cliente evidências sobre a conformidade do Suboperador com as Medidas Técnicas e Organizacionais.

viii. A Sinch funcionará de acordo com os princípios de proteção de dados desde o projeto e por padrão e deverá fornecer documentação suficiente da implementação da proteção de dados desde o projeto e por padrão.

2 Medidas Organizacionais

A organização interna do operador de dados deverá atender aos requisitos específicos de proteção de dados.

A. Políticas e Gerenciamento de Políticas

i. A SINCH deverá ter um sistema de gestão de segurança da informação (ISMS) definido e documentado, incluindo uma política e procedimentos de segurança da informação em vigor, que deverão ser aprovados pela administração da SINCH. Eles deverão ser publicados dentro da organização da SINCH e comunicados as pessoas relevantes da SINCH.

ii. A SINCH deverá rever periodicamente as políticas e procedimentos da SINCH relativos à proteção de dados e segurança da informação e atualizá-los, se necessário, para garantir a sua conformidade com as Medidas Técnicas e Organizacionais e o DPA.

B. Organização de Proteção de Dados e Segurança da Informação

i. A SINCH deverá indicar pelo menos um encarregado pelo tratamento de dados pessoais com as competências adequadas e que atua como o principal contacto para a proteção de dados. Se exigido por lei, a SINCH nomeará um encarregado de proteção de dados em nível de empresa.

ii. A SINCH deverá ter funções e responsabilidades de segurança definidas e documentadas em sua organização.

C. Requisitos Organizacionais

i. A SINCH deverá garantir que o pessoal da SINCH trate as informações de acordo com o nível de confidencialidade exigido pelo DPA e que tenha o compromisso por escrito dos funcionários de manter a confidencialidade.

ii. A SINCH deverá garantir que as pessoas relevantes da Sinch estejam cientes do uso aprovado (incluindo restrições de uso, conforme o caso) de informações, instalações e sistemas nos termos do DPA.

iii. A SINCH deverá garantir que qualquer pessoal da SINCH que desempenhe atribuições nos termos do DPA seja confiável, atenda aos critérios de segurança estabelecidos e tenha sido, e durante o prazo da atribuição, sujeito a uma triagem adequada e verificação de antecedentes (se permitido pela lei aplicável).

iv. A SINCH deverá garantir que o pessoal da SINCH com responsabilidades de segurança seja adequadamente treinado para realizar as tarefas relacionadas à segurança.

v. A SINCH deverá fornecer ou garantir treinamento periódico de conscientização para o pessoal relevante da SINCH. Esse treinamento SINCH deverá incluir, sem limitação:

a) Como lidar com a segurança da informação do Cliente (ou seja, a proteção da confidencialidade, integridade e disponibilidade da informação);
b) Porque a segurança da informação é necessária para proteger as informações e sistemas dos clientes;
c) Os tipos comuns de ameaças à segurança (como roubo de identidade, malware, *hacking*, vazamento de informações e ameaça interna);
d) A importância de cumprir as políticas de segurança da informação e aplicar os padrões/procedimentos associados;
e) Responsabilidade pessoal pela segurança da informação (como proteger as informações relacionadas à privacidade do Cliente e relatar violações de dados reais e suspeitas).

3 Confidencialidade

A. Controle de Acesso (Segurança física e ambiental)

i. A SINCH deverá proteger as instalações de tratamento de informações contra ameaças e riscos externos e ambientais, incluindo falhas de energia/cabeamento e outras interrupções causadas por falhas no suporte aos serviços públicos. Isso inclui perímetro físico e proteção de acesso.
ii. A SINCH deverá proteger os bens contra roubo, manipulação e destruição.
iii. A SINCH deverá especificar os indivíduos autorizados permitidos em suas instalações de tratamento e ter um processo de controle de acesso.
iv. Medidas adicionais para Data Centers:
a) Todos os Data Centers aderem a procedimentos de segurança rígidos apoiados por guardas, câmeras de vigilância, detectores de movimento, mecanismos de controle de acesso e outras medidas para evitar que os equipamentos e as instalações do data center sejam comprometidos.
b) Apenas representantes autorizados têm acesso aos sistemas e infraestrutura dentro das instalações do Data Center.
c) Para proteger a funcionalidade adequada, os equipamentos de segurança física (por exemplo, sensores de movimento, câmeras etc.) passam por manutenção regularmente.
d) A SINCH e todos os provedores de Data Centers terceirizados registram os nomes e horários do pessoal autorizado que entra nas áreas privadas da SINCH dentro dos Data Centers.

B. Controle de acesso (Lógico)

i. A SINCH deverá ter uma política de controle de acesso definida e documentada para instalações, sites, rede, sistema, aplicativo e acesso a informações/dados (incluindo controles de acesso físico, lógico e remoto), um processo de autorização para acesso de usuário e privilégios, procedimentos para revogar acesso direitos e um uso aceitável de privilégios de acesso para o pessoal da SINCH no local.
ii. A SINCH deverá ter um registro de usuário formal e documentado e um processo de cancelamento de registro implementado para permitir a atribuição de direitos de acesso.
iii. A SINCH deverá ter um processo de *joiner-mover-leaver* para seus funcionários.
iv. A SINCH deverá atribuir todos os privilégios de acesso com base no princípio da necessidade de tomar conhecimento e no princípio do menor privilégio.
v. A SINCH deverá usar autenticação forte (multifatorial) para usuários de acesso remoto e usuários que se conectam a partir de uma rede não confiável.

vi. A SINCH deverá garantir que o pessoal da SINCH tenha um identificador pessoal e único (ID do usuário) e use uma técnica de autenticação adequada, que confirma e garante a identidade dos usuários.

C. Criptografia/Pseudonimização/Anonimização

i. A SINCH deverá garantir o uso adequado e eficaz da criptografia nas informações classificadas como confidenciais e secretas (como dados pessoais).
ii. A SINCH deverá proteger as chaves criptográficas e armazená-las de acordo com a legislação aplicável.
iii. A SINCH implementará medidas adequadas para pseudonimização (substituição de identificadores pessoais por informações não pessoais) quando adequado.
iv. A SINCH implementará medidas adequadas para anonimato (desidentificar identificadores pessoais com informações não pessoais) quando adequado.

D. Diretrizes sobre a admissão nas instalações do Cliente e/ou instalações SINCH

A autorização de acesso às instalações e propriedades (como edifícios de datacenter, edifícios de escritórios, locais técnicos) está sujeita ao seguinte:

i. A SINCH deverá seguir os regulamentos locais (como regulamentos para "áreas restritas") para as instalações do Cliente ao realizar as cessões nos termos do Contrato.
ii. O pessoal da SINCH deverá portar carteira de identidade ou, no caso de visitantes, um crachá de visitante, visível o tempo todo durante o trabalho.
iii. Após o emprego ou conclusão da tarefa, ou quando o pessoal da SINCH é transferido para outras tarefas, o pessoal deverá, sem demora, informar o pessoal autorizado da mudança e devolver quaisquer chaves, cartões-chave, certificados, crachás de visitante e itens semelhantes.
iv. Chaves ou cartões-chave deverão ser assinados pessoalmente pelo pessoal da SINCH e deverão ser manuseados de acordo com as regras escritas dadas no recebimento.
v. A perda da chave ou do cartão-chave deverá ser comunicada sem demora ao pessoal autorizado.
vi. Fotografar dentro ou nas instalações sem permissão é proibido.
vii. Bens não deverão ser removidos das instalações sem permissão.
viii. O pessoal da SINCH não deverá permitir o acesso de pessoas não autorizadas às instalações.

4 Segurança das operações

i. A SINCH deverá ter um sistema de gerenciamento de mudanças estabelecido para fazer mudanças nos processos de negócios, instalações e sistemas de tratamento de informações. O sistema de gerenciamento de mudanças deverá incluir testes e revisões antes que as mudanças sejam implementadas, tais como procedimentos para lidar com mudanças urgentes, procedimentos de reversão para se recuperar de mudanças que falharam, logs que mostram o que foi alterado, quando e por quem.
ii. A SINCH implementará proteção contra malware para garantir que qualquer software usado para o fornecimento dos Serviços da SINCH ao Cliente seja protegido contra malware.
iii. A rede da SINCH é protegida da rede pública por firewalls.
iv. A SINCH deverá fazer cópias de backup de informações críticas e testar cópias de backup para garantir que as informações possam ser restauradas conforme acordado com o Cliente.
v. A SINCH deverá registrar e monitorar as atividades, como criar, ler, copiar, alterar e excluir os dados tratados, bem como exceções, falhas e eventos de segurança da informação e revisá-los regularmente. Além disso, a SINCH deverá proteger e armazenar (por pelo menos 6 meses ou durante o(s) período(s) definido(s) pela Legislação de Proteção de Dados) informações de registro e, mediante solicitação, fornecer dados de monitoramento ao Cliente. Anomalias/incidentes/indicadores de comprometimento deverão ser reportados de acordo com os requisitos de gestão de violação de dados conforme estabelecido abaixo.
vi. A SINCH deverá gerenciar vulnerabilidades de todas as tecnologias relevantes, como sistemas operacionais, bancos de dados, aplicativos de forma proativa e em tempo hábil.
vii. A SINCH deverá estabelecer linhas de base de segurança (reforço) para todas as tecnologias relevantes, como sistemas operacionais, bancos de dados, aplicativos.
viii. A SINCH deverá garantir que o desenvolvimento seja segregado do ambiente de teste e produção.

5 Integridade

i. A SINCH deverá implementar controles de segurança de rede, como nível de serviço, firewall e segregação para proteger os sistemas de informação.
ii. A SINCH opera um sistema de detecção de phishing e SPAM com o objetivo de proteger seus clientes e a SINCH (e os Dados Pessoais dos quais as partes são o Controlador) contra conteúdo indesejado e a propagação de SPAM/phishing e cumprir os requisitos do operador e a legislação aplicável. O sistema recupera a(s) URL(s) do corpo da mensagem de solicitação encerrada por dispositivo móvel e, em seguida, habilita a validação da URL emitindo uma solicitação de método GET para a URL e expandindo para a URL completa como se estivesse na barra de endereço do navegador. Se necessário, devido a informações insuficientes ou suspeita de conteúdo não conforme, toda a página poderá ser carregada e analisada, incluindo o conteúdo dessa página. Este é um algoritmo de *machine learning* (com validação humana) projetado para aprender com a detecção de phishing e SPAM confirmados e que os dados

serão usados para essa finalidade dentro do grupo SINCH. A SINCH não fornecerá nem enviará dados pessoais dos quais o Cliente é o controlador para terceiros fora do Grupo SINCH, exceto para os Suboperadores necessários para fornecer esta funcionalidade.

iii. Os Dados Pessoais tratados em nome deverão ser tratados exclusivamente de acordo com o Contrato e as instruções do controlador para o operador.

iv. A SINCH trabalhará de acordo com instruções escritas ou acordos e documentos pertencentes a esse DPA.

6 Gerenciamento de violação de dados

i. A SINCH deverá ter estabelecido procedimentos para gerenciamento de violação de dados.

ii. A SINCH informará o Cliente sobre qualquer violação de dados (incluindo, mas não se limitando a incidentes relacionados ao tratamento de dados pessoais) o mais rápido possível, mas o mais tardar em 72 horas após a violação de dados ter sido identificada.

iii. Todos os relatórios de incidentes relacionados à segurança deverão ser tratados como informações confidenciais e criptografados, usando métodos de criptografia padrão da indústria.

iv. O relatório de violação de dados deverá conter pelo menos as seguintes informações:

a) A natureza da violação de dados,
b) A natureza dos dados pessoais afetados,
c) As categorias e o número de titulares de dados em questão,
d) O número de registros de dados pessoais em questão,
e) As medidas tomadas para lidar com a violação de dados,
f) As possíveis consequências e efeitos adversos da violação de dados, e
g) Qualquer outra informação que o Cliente seja obrigado a relatar ao regulador relevante ou titular dos dados.

Na medida do legalmente possível, a SINCH poderá reivindicar compensação por serviços de suporte nos termos desta cláusula que não sejam atribuíveis a falhas por parte da SINCH.

7 Gestão de Continuidade dos Negócios

i. A SINCH deverá identificar os riscos de continuidade dos negócios e tomar as medidas necessárias para controlar e mitigar esses riscos.

ii. A SINCH deverá ter processos e rotinas documentados para lidar com a continuidade dos negócios.

iii. A SINCH deverá garantir que a segurança da informação seja incorporada aos planos de continuidade de negócios.

iv. A SINCH deverá avaliar periodicamente a eficiência de sua gestão de continuidade de negócios e a conformidade com os requisitos de disponibilidade (se houver).

8 Desenvolvimento e manutenção de sistema/software (quando o desenvolvimento de software ou desenvolvimento de sistema é fornecido ao Cliente pela SINCH)

i. A SINCH deverá implementar regras para o ciclo de vida de desenvolvimento de software e sistemas, incluindo procedimentos de mudança e revisão.

ii. A SINCH deverá testar a funcionalidade de segurança durante o desenvolvimento em um ambiente controlado.

iii. A gestão de patch de segurança é implementada para fornecer implantação regular e periódica de atualizações de segurança relevantes.

iv. A SINCH trabalhará de acordo com os princípios de proteção de dados "*by design & by* default" e deverá fornecer documentação suficiente da implementação da proteção de dados "*by design & by default"*.

Anexo 2 do Contrato de proteção de dados – REGRAS ESPECÍFICAS com base na legislação nacional aplicável

1. Espanha

Caso o Controlador/Operador esteja situado na Espanha, as medidas técnicas e organizacionais a serem tomadas pelo Operador estão sujeitas às leis de proteção de dados da Espanha. Neste caso, o preâmbulo do Anexo 1 deste DPA deverá ser complementado da seguinte forma:

"O Operador deverá certificar-se de que as seguintes medidas técnicas e organizacionais estão em conformidade com as medidas de "segurança de alto nível" de acordo com o Real Decreto Espanhol 1720/2007 Título VIII, Art. 80 ff. O operador deverá implementar, em particular, os requisitos da seção três (Art. 89 e seguintes) do Real Decreto Espanhol 1720/2007, caso os requisitos deste Anexo 1 não estejam em conformidade com esses requisitos. Neste caso, o Operador deverá informar o Controlador e apresentar quaisquer alterações ou desvios deste Anexo 1 que julgar necessário para uma aprovação prévia do Controlador."

2. Canadá

A definição de "Dados Pessoais Sensíveis" na Cláusula 1 deste DPA será considerada da seguinte forma:

"Dados Pessoais Sensíveis" significam informações sobre origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação a sindicatos, saúde ou vida sexual ou qualquer outro pessoal que possa ser considerado como dado sensível com base na legislação aplicável."

Além do que é acordado neste DPA, será aplicável em relação à transferência de dados:

"O Controlador reconhece que o Operador poderá transferir, armazenar e tratar Dados Pessoais para territórios fora do Canadá, onde estarão sujeitos às leis das jurisdições estrangeiras nas quais são mantidos. O Operador não deverá, e deverá certificar-se de que qualquer Afiliada ou qualquer terceiro com quem contrate para Tratar Dados Pessoais em seu nome em conexão com o(s) Serviço(s) relevante(s), não:

- transferir Dados pessoais para um território fora do Canadá, exceto em termos substancialmente semelhantes aos termos aqui, que são acordados antes de tal transferência; ou
- operar em relação a esses Dados Pessoais de qualquer forma que coloque o Controlador em violação de suas obrigações de acordo com as leis de privacidade aplicáveis."

Além do que é acordado neste DPA:

"O Controlador reconhece que possui todos os consentimentos necessários e autoridade legal dos titulares dos dados que permitiriam ao Operador tratar os dados."

Além do que é acordado na Seção 7 deste DPA:

"As partes também cooperarão com relação a quaisquer notificações de violação de dados às autoridades regulatórias canadenses, indivíduos e outras organizações que sejam exigidas por lei ou de outra forma aconselháveis a critério exclusivo do Controlador."

Sem limitar os termos e condições do DPA para o Canadá e do Contrato, na medida em que seja aplicável no Canadá, o seguinte se aplica:

"O Operador obedecerá a toda a legislação canadense federal e provincial de privacidade e AntiSpam aplicável ao Controlador e ao Operador no curso do tratamento de quaisquer Dados em conexão com os Serviços, incluindo todos os requisitos aplicáveis de notificação, consentimento, conteúdo e cancelamento de assinatura em relação ao envio de mensagens eletrônicas e a instalação de programas de computador no dispositivo de outra pessoa.

O Operador providenciará que o acesso aos Dados seja limitado apenas aos funcionários e agentes autorizados do Operador que precisam ter acesso aos Dados Pessoais exclusivamente para fins de processamento dos Serviços pelo Operador."

3. Austrália

Seguindo as diretrizes australianas de proteção de dados (Princípios de Privacidade Australianos; APP) do Anexo 1 da "Emenda de Privacidade (Aprimorando a Proteção de Privacidade) Lei 2012", que é um suplemento da "Lei de Privacidade de 1988", o seguinte é aplicável ao tratamento de Dados Pessoais:

(i) "**Controlador**" significa uma pessoa que, sozinha ou em conjunto com outras pessoas, estabelece os objetivos e a forma de tratamento dos dados pessoais; e "**Operador**" significa qualquer pessoa (que não seja um funcionário do Controlador) que, em nome do Controlador, trata dados pessoais.

(ii) Quando um Controlador ou seus Usuários Autorizados na Austrália pretendem coletar Dados Pessoais no Serviço em Nuvem, o Controlador se compromete a obter o consentimento prévio de cada Sujeito de Dados a uma Transferência Internacional de acordo com este Cronograma se, e na medida em que for necessário de acordo com a Lei de Privacidade. O Controlador, por meio deste, confirma que recebeu os dados pessoais e informou as pessoas interessadas sobre a divulgação dos dados pessoais de acordo com o APP e a Lei de Privacidade de 1988. Com base nisso, a exigência de "Consentimento Livre e Esclarecido" no item 8.1 do APP é considerada cumprida devido à exceção do "Consentimento Livre e Esclarecido". Desde que o Consentimento Informado não se aplique, este Cronograma fornece a estrutura para a proteção dos Dados Pessoais das pessoas afetadas na Austrália, na medida em que fornece pelo menos essencialmente a mesma privacidade que o APP, e o Operador e seus Suboperadores se comprometem a um nível de proteção de dados que é o mesmo que o estabelecido nas Seções 2, 3 e 6 deste anexo (exceção de "Lei Substancialmente Semelhante" sob o APP 8.2 (a)). Com isso, vê-se como cumprido o requisito estabelecido no APP 8.1 de "Lei Substancialmente Similar" para esse fim.

4. Reino Unido

Na medida em que uma Lei de Proteção de Dados (incluindo o novo Regulamento Básico de Proteção de Dados da União Europeia ou seu sucessor depois que Grã-Bretanha deixar a União Europeia) entrar em vigor após a data de entrada em vigor deste DPA e for contrário aos termos deste DPA ou caso contrário exija uma alteração a este DPA, uma parte poderá notificar a outra parte a fim de começar a negociar as alterações necessárias a este DPA de acordo com o princípio da boa-fé.

5. Suíça

De acordo com o art. 3 lit. b da Lei Federal Suíça de 19 de junho de 1992 sobre Proteção de Dados (FADP), as definições na cláusula 1 deste DPA deverão ser consideradas conforme segue:
"**Titular dos Dados**": pessoas físicas ou jurídicas cujos dados são tratados.

6. Itália

De acordo com o Artigo 29 do Código Italiano de Proteção de Dados Pessoais, é necessário indicar o operador de dados em conformidade com a lei italiana e descrever as tarefas específicas que eles têm de acordo com o Código Italiano de Proteção de Dados. Ao assinar este DPA, o Controlador indica o Operador como Operador de Dados. O Operador de Dados deverá tratar os dados de acordo com os regulamentos e medidas de segurança previstos no Decreto Legislativo no. 196/2003 e identificados no Anexo B do mesmo "Especificações técnicas relativas às medidas mínimas de segurança" e os regulamentos e medidas de segurança que serão fornecidos como atualizações para aqueles aqui contidos. As medidas a serem tomadas estão descritas neste DPA e seus Anexos.

Especificamente, o Operador de Dados concorda em desempenhar suas funções estritamente de acordo com as Instruções que lhe forem fornecidas pelo Controlador de Dados, e deverá, nos termos do art. 29, parágrafo 5º do Decreto Legislativo nº. 196/2003, supervisionar o cumprimento tempestivamente das tarefas atribuídas ao Operador de Dados.

O Operador de Dados compromete-se a:

- fornecer os serviços de Tratamento de Dados descritos no DPA, comprometendo-se particularmente a concluir qualquer operação de tratamento ou conjunto de operações, com ou sem o auxílio de meios eletrônicos, no que diz respeito à coleta, registro, organização, armazenamento, consulta, tratamento, modificação, seleção, extração, comparação, uso, interconexão, bloqueio, comunicação, disseminação, cancelamento e destruição de dados, mesmo que não registrados em banco de dados;
- executar os Serviços de acordo com os requisitos de proteção de dados e apenas para os fins pretendidos, conforme descrito no DPA. O Operador de Dados é obrigado a salvaguardar o sigilo dos dados de acordo com a Legislação de Proteção de Dados, particularmente o Operador de Dados compromete-se a concluir as operações de tratamento de dados aqui referidas de uma forma legal e adequada, que preveja a máxima confidencialidade e que também preveja atempadamente e total conformidade com as leis e regulamentos aplicáveis;
- aplicar medidas para que todo o pessoal encarregado do manuseio de dados o faça em conformidade com as leis e regulamentos em vigor, bem como quaisquer Instruções neles fornecidas;
- fiscalizar se o seu tratamento de dados pessoais obedece aos requisitos estabelecidos pelo Decreto Legislativo nº 196/2003,

- armazenar os dados pessoais coletados em conformidade com as medidas de segurança previstas no art. 31 et seq. do Decreto Legislativo 196/2003, garantindo a observância das medidas mínimas de segurança.

Tanto o Controlador como o Operador reconhecem que as Medidas Técnicas e Organizacionais do Anexo 1 do DPA são atualmente suficientes para cumprir as medidas dos art. 31 e seguintes. do Decreto Legislativo 196/2003.

Se necessário, um administrador do sistema será nomeado em uma carta de nomeação separada para o administrador do sistema.

7. Estados Unidos da América (EUA)

As seguintes definições na cláusula 1 deste DPA deverão ser consideradas da seguinte forma:

"Dados Pessoais (nos EUA, é usado o termo Informações de Identificação Pessoal): qualquer elemento individual de informação referente às circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável;

Dados confidenciais (também conhecidos como "Dados Pessoais Sensíveis"): informações sobre origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação a sindicatos, saúde ou vida sexual, número de segurança social, número de carteira de motorista ou estado ou emite federalmente o número do cartão de identificação, número da conta ou número do cartão de crédito ou débito, ou um número da conta em combinação com qualquer código de segurança exigido, código de acesso ou senha que permitiria o acesso à conta financeira de um indivíduo ou qualquer outra informação cuja divulgação não autorizada que poderá exigir que o Controlador notifique os indivíduos afetados."

8. Singapura

Caso o Controlador esteja situado em Singapura, o seguinte texto será adicionado à cláusula 4 deste DPA:

"O Operador cumprirá em tempo hábil com as instruções ou decisões de qualquer autoridade competente de proteção de dados e privacidade em relação aos Dados. O Operador prestará ao Controlador a cooperação, assistência e informações que o Controlador razoavelmente solicitar para cumprir com suas obrigações de acordo com a Legislação de Proteção de Dados."

9. Malásia

Caso o Controlador esteja situado na Malásia, a definição de categorias especiais de dados ("Dados Pessoais Sensíveis" significa informações sobre origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, saúde ou sexo vida) na cláusula 1 deste DPA (Definições) será substituída pelo seguinte: "Dados Pessoais Sensíveis" significa informações sobre origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, associação a sindicatos, prática ou alegada prática de qualquer delito, saúde física ou mental ou vida sexual."

Caso o Controlador esteja situado na Malásia, o seguinte texto da cláusula 8 deste DPA será complementado com "O Operador implementará as medidas técnicas e organizacionais conforme especificado na Legislação de Proteção de Dados e no Anexo 1 para proteger os Dados contra acidentes ou destruição ilegal ou perda acidental, alteração, divulgação não autorizada, uso ou acesso e contra todas as outras formas ilegais de processamento ".

Caso o Controlador esteja situado na Malásia, o seguinte texto será adicionado à cláusula 9.1(b) deste DPA:

"Ambas as Partes comprometem-se a guardar sigilo sobre todas as informações adquiridas no âmbito do Contrato e deste DPA, especialmente no que se refere aos Dados, tendo em consideração o segredo do Controlador. Esta obrigação continua a aplicar-se após a rescisão do DPA."

Caso o Controlador esteja situado na Malásia, o seguinte texto será adicionado à cláusula 11 deste DPA "O relatório cobrirá os objetivos das medidas técnicas e organizacionais estabelecidas no Anexo 1 e na Legislação de Proteção de Dados."

10. Índia

As seguintes definições na cláusula 1 deste DPA deverão ser alteradas da seguinte forma:
"**Dados Pessoais**" significa qualquer elemento individual de informação sobre as circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável. Informação pessoal, que é qualquer informação que diga respeito a uma pessoa singular, que, direta ou indiretamente, em combinação com outra informação disponível ou susceptível de estar disponível com uma pessoa jurídica, é capaz de identificar essa pessoa.

"**Dados Pessoais Sensíveis**" significa dados pessoais confidenciais ou informações de uma pessoa; isto significa tais informações pessoais que consistem em informações relacionadas a;—(i) senha; (ii) informações financeiras, como conta bancária ou cartão de crédito ou cartão de débito ou outros detalhes de instrumento de pagamento; (iii) estado de saúde física, fisiológica e mental; (iv) orientação sexual; (v) registros médicos e histórico; (vi) informações biométricas; (vii) qualquer detalhe relacionado às cláusulas acima, conforme fornecido a pessoa jurídica para a prestação de serviço; e (viii) qualquer uma das informações recebidas nos termos das cláusulas acima por pessoa jurídica para tratamento, armazenada ou tratada sob contrato legal ou de outra forma: desde que, qualquer informação que esteja livremente disponível ou acessível em domínio público ou fornecida de acordo com a Lei de Direito à Informação, 2005 ou qualquer outra lei em vigor não serão considerados dados ou informações pessoais sensíveis para os efeitos destas regras.

O seguinte texto será adicionado à cláusula 8 deste DPA:

"O Operador deverá cumprir as práticas e procedimentos de segurança razoáveis prescritos pelo Controlador e/ou a política de privacidade do Controlador deverá constituir práticas e procedimentos de segurança razoáveis de acordo com a seção 43A da Lei de Tecnologia da Informação (indiana) de 2000 e as regras emitidas pelo governo indiano ao abrigo de tal disposição, portanto, não será aplicável."

11. China

O seguinte texto será adicionado à cláusula 16 deste DPA:

"A responsabilidade legal de acordo com as leis da República Popular da China poderá ser aplicável dependendo dos acordos do Controlador com seu cliente."

12. Brasil

As seguintes definições na cláusula 1 deste DPA deverão ser alteradas da seguinte forma:

"Dados Pessoais Sensíveis" "significam dados pessoais sensíveis: isso significa tais dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

"**Tratamento de Dados"** significa toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

Caso os suboperadores estejam situados no Brasil, as obrigações dispostas pelas cláusulas 7.2, 7.4 e 7.5 deste DPA não serão aplicáveis.

13. Colombia

Além do que foi acordado na cláusula 8 e na cláusula 15 deste DPA, aplica-se o seguinte, em relação ao tratamento e transferência de Dados Pessoais:
"O Controlador reconhece que o Operador pode transferir, armazenar e tratar Dados Pessoais em territórios fora da Colômbia, de forma que os dados estarão sujeito às leis das jurisdições estrangeiras em que são armazenados. O controlador reconhece que possui todos os consentimentos necessários e autoridade legal concedidas pelos titulares de dados, bem como registros de bancos de dados que possibilitam o Operador a tratar os dados dentro dos bancos de dados e em países que asseguram, minimamente, o mesmo padrão de proteção de dados (nível adequado de proteção) àquele assegurado na legislação colombiana (tais como, mas não limitadas ao Decreto nº 90 de 2018, a Circular Única da Superintendência da Indústria e Comércio e a Circular Externa N° 005 de 2017 da Superintendência da Indústria e Comércio).

14. Argentina

Além do que foi acordado na cláusula 8 e na cláusula 15 deste DPA. as Partes concordam em realizar as seguintes Cláusulas Contratuais-Tipo Argentinas, para transferência internacional, desde que o Controlador dos Dados Pessoais ser da Argentina e/ou a Legislação de Proteção de Dados aplicável e/ou a Autoridade de Proteção de Dados Argentina exigirem que estas cláusulas sejam realizadas.

Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios

Entre, por una parte, _____, con domicilio en la calle_____, localidad_____, provincia de _____, Argentina, (en adelante, "el exportador de datos") y, por la

otra, _____ (nombre), _____ (dirección y país), (“en adelante, el importador de datos”), en conjunto “las partes”, convienen el presente contrato de transferencia internacional de datos personales para la prestación de servicios, sometiéndola a los términos y condiciones que se detallan a continuación.