ACORDO DE PROCESSAMENTO DE DADOS

Este Acordo de processamento de dados (o "Acordo") é firmado entre a Siemens Product Lifecycle Management Software Inc., também conhecida como Siemens Industry Software (doravante denominada "SISW") e o cliente que assinou sua aceitação dos termos e condições deste Acordo ("Cliente"). SISW retém o direito de utilizar suas empresas afiliadas para fazer valer qualquer um de seus direitos e cumprir com todas as obrigações deste Acordo. Portanto, o termo "SISW" utilizado neste documento também pode se referir às empresas afiliadas que são direta ou indiretamente controladas ou de propriedade da principal empresa da Siemens Product Lifecycle Management Software Inc. e que tenham sido autorizadas pela Siemens Product Lifecycle Management Software Inc. para distribuir os serviços de nuvem da SISW (o "Serviço de nuvem").

O Cliente deve ser exclusivamente responsável por determinar o tipo de dados e os indivíduos afetados pelo processamento, e deve garantir a legitimidade desse processamento por meio do Serviço de nuvem. O Cliente também deve ser responsável por qualquer correção, exclusão ou bloqueio de dados pessoais, usando as funcionalidades oferecidas pelo Serviço de nuvem. O Cliente pode exportar e excluir seus dados, incluindo dados pessoais, usando as funcionalidades oferecidas pelo Serviço de nuvem. Após a rescisão deste Acordo de processamento de dados, o Cliente deve ter 30 dias para enviar uma solicitação por escrito à SISW para que os Dados do cliente sejam disponibilizados por download para o Cliente. Após o vencimento de qualquer período estabelecido pela SISW em resposta a tal solicitação, quaisquer dados restantes do Cliente estarão sujeitos à exclusão e não estarão mais disponíveis ao Cliente. A SISW e o Cliente concordam que, dentro do escopo do Serviço de nuvem, o direito do Cliente de emitir instruções será exercido exclusivamente por meio do uso das funcionalidades oferecidas pelo Serviço de nuvem. Instruções adicionais relativas aos dados do Cliente exigem um acordo por escrito separado entre a SISW e o Cliente, incluindo um acordo sobre quaisquer taxas adicionais a serem pagas pelo Cliente para a realização de tais instruções. O Cliente se compromete a não transferir nem armazenar informações de saúde protegidas (PHI) no Serviço de nuvem, a não ser que a SISW e o Cliente tenham entrado em um acordo por escrito, separado, que permita expressamente o armazenamento de PHI no Serviço de nuvem.

Ao fornecer o Serviço de nuvem, em relação ao sistema de produção, a SISW deve seguir as medidas técnicas e organizacionais descritas no Apêndice 2, Anexo A, deste Acordo de processamento de dados. Sistemas que não sejam de produção, relacionados ao Serviço de nuvem, podem ou não seguir as medidas descritas no Apêndice 2, Anexo A. Além disso, a SISW pode alterar as medidas técnicas e organizacionais aplicáveis ao sistema de produção de tempos em tempos, considerando que tais alterações não afetem negativamente o nível de proteção fornecido por tais medidas de forma substancial. A SISW irá restringir seu pessoal de coletagem, processamento ou de uso de dados pessoais sem autorização, e irá empregar apenas pessoal no processamento de dados do Cliente que tenha sido especificamente instruído em conformidade com os requisitos de proteção da privacidade dos dados.

A SISW deve ter o direito de envolver subprocessadores no desempenho do Serviço de nuvem. Até o ponto em que o acesso dos subprocessadores aos dados pessoais do Cliente não pode ser excluído, a SISW irá fornecer ao Cliente, mediante solicitação, uma lista desses subprocessadores e suas respectivas localizações, e irá atualizar essa lista, conforme necessário, antes de qualquer novo subprocessador receber acesso aos dados pessoais do Cliente. No caso de o Cliente apresentar uma objeção razoável a qualquer novo subprocessador, o Cliente deve informar à SISW sobre essa objeção e, se a SISW insistir no envolvimento do novo subprocessador, ele deve ter o direito de rescindir este Acordo de processamento de dados por justa causa. Até o ponto em que o envolvimento de um subprocessador qualquer envolva a transferência de dados pessoais através de fronteiras, a SISW irá se esforçar para fazer com que esse subprocessador mantenha um nível adequado de proteção desses dados pessoais.

A SISW irá verificar regularmente a adesão às medidas técnicas e organizacionais aplicáveis e irá, mediante solicitação razoável por parte do Cliente, confirmar ao cliente que as medidas técnicas e organizacionais aplicáveis estão sendo seguidas. No caso de o Cliente ter motivo para acreditar que a confirmação emitida pela SISW está errada, o Cliente deve ter o direito de confirmar a adesão às medidas organizacionais e técnicas através do agendamento de uma auditoria com a SISW, sujeita a um aviso prévio razoável. Essa auditoria deve ser realizada à custa e despesa do Cliente.

A SISW e o Cliente concordam que quaisquer transferências de dados pessoais do Cliente a partir de países da União Europeia para países de fora da UE, que a UE considere não ter um nível adequado de proteção de dados pessoais, serão conduzidas de acordo com as cláusulas contratuais padrão da UE, que estão definidas no Anexo A e são inteiramente incorporadas neste documento. No caso de um conflito entre os termos deste Acordo de processamento de dados e os termos das cláusulas contratuais padrão, as cláusulas contratuais padrão irão prevalecer. As cláusulas contratuais padrão serão regidas pelas leis do estado membro da UE em que o exportador de dados (conforme definição no Anexo A) estiver estabelecido.

Anexo A
Cláusulas contratuais padrão da UE

Para os propósitos do Artigo 26(2) da Diretriz 95/46/EC para a transferência de dados pessoais a processadores estabelecidos em outros países que não garantem um nível adequado de proteção dos dados

por e entre

o Cliente e/ou uma empresa afiliada do Cliente baseada na UE

(doravante o "**exportador de dados**")

e

a Siemens Product Lifecycle Management Software Inc., também conhecida como Siemens Industry Software, incluindo quaisquer empresas afiliadas que são direta ou indiretamente controladas ou de propriedade da principal empresa da Siemens Product Lifecycle Management Software Inc. e que tenham sido autorizadas pela Siemens Product Lifecycle Management Software Inc. a processar dados em seu nome

(doravante, o "**importador de dados**")

cada um individualmente sendo uma "parte"; e coletivamente "as partes",

CONCORDARAM com as seguintes Cláusulas contratuais (as Cláusulas) para fornecer proteções adequadas em relação à proteção de privacidade e direitos fundamentais e liberdades de indivíduos para a transferência pelo exportador de dados ao importador de dados pessoais especificados no Apêndice 1.

Seção 1. Definições

Para os propósitos das Cláusulas:

(a) 'dados pessoais', 'categorias especiais de dados', 'processo/processamento', 'controlador', 'processador', 'assunto dos dados' e 'autoridade de supervisão' devem ter o mesmo significado conforme a Diretriz 95/46/EC do Parlamento Europeu e do Conselho de 24 de outubro de 1995 na proteção de indivíduos em relação ao processamento de dados pessoais no livre movimento desses dados ;

(b) 'o 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, dados pessoais a serem processados em seu nome depois da transferência, de acordo com suas instruções e com os termos das Cláusulas e quem não está sujeito a um sistema de um país terceiro que garanta proteção adequada dentro do significado do Artigo 25(1) da Diretriz 95/46/EC;

(d) 'o subprocessador' significa qualquer processador envolvido pelo importador de dados ou por qualquer outro subprocessador do importador de dados que concorda em receber, do importador de dados ou de qualquer outro subprocessador do importador de dados, dados pessoais exclusivamente destinados ao processamento de atividades a serem realizadas em nome do exportador de dados depois da transferência, de acordo com suas instruções, com os termos das Cláusulas e com os termos do subcontrato redigido;

(e) 'a lei de proteção de dados aplicável' significa que a legislação que protege os direitos fundamentais e as liberdades dos indivíduos e, em particular, seus direitos à privacidade com respeito ao processamento de dados pessoais aplicáveis a um controlador de dados no Estado Membro em que o exportador de dados está estabelecido;

(f) 'medidas de segurança organizacional e técnica' significam as medidas feitas para proteger dados pessoais contra destruição acidental ou de má fé, alteração, revelação não autorizada ou acesso, principalmente quando o processamento envolver a transmissão de dados através de uma rede, e contra todas as outras formas ilegais de processamento.

Seção 2. Detalhes da transferência

Os detalhes da transferência e, em particular, as categorias especiais de dados pessoais, quando aplicáveis, são especificadas no Apêndice 1, que é parte integrante das Cláusulas.

Seção 3. Cláusula de beneficiário terceiro

1. O titular dos dados pode aplicar contra o exportador de dados esta Cláusula, Cláusula 4(b) a (i), Cláusula 5(a) a (e), e (g) a (j), Cláusula 6(1) e (2), Cláusula 7, Cláusula 8(2) e Cláusulas 9 a 12 como beneficiário terceiro.

2. O titular dos dados pode aplicar contra o exportador de dados esta Cláusula, Cláusula 5(a) a (e) e (g), Cláusula 6, Cláusula 7, Cláusula 8(2) e Cláusulas 9 a 12, em casos em que o exportador de dados tenha factualmente desaparecido ou tenha deixado de existir segundo a lei, a não ser que qualquer entidade sucessora tenha assumido todas as obrigações legais do exportador de dados por contrato ou por operação de lei, e em resultado disso, tenha assumido os direitos e obrigações do exportador de dados, em cujo caso o titular dos dados pode impor as cláusulas acima contra a referida entidade.

3. O titular dos dados pode aplicar contra o subprocessador esta Cláusula, Cláusula 5(a) a (e) e (g), Cláusula 6, Cláusula 7, Cláusula 8(2) e Cláusulas 9 a 12, em casos em que o exportador de dados e o importador de dados tenham factualmente desaparecido ou tenha deixado de existir segundo a lei, ou tenha falido, a não ser que qualquer entidade sucessora tenha assumido todas as obrigações legais do exportador de dados por contrato ou por operação de lei, e em resultado disso, tenha assumido os direitos e obrigações do exportador de dados, em cujo caso o titular dos dados pode aplicar as cláusulas acima contra a referida entidade. Essa responsabilidade de terceiros do subprocessador deve ser limitada a suas próprias operações de processamento diante das Cláusulas.

4. As partes não fazem objeção a um titular de dados sendo representado por uma associação ou outra organização, se o titular dos dados assim desejar expressamente e se isso for permitido por lei nacional.

Seção 4. Obrigações do exportador de dados

O exportador de dados concorda e garante:

(a) que o processamento, incluindo a transferência propriamente dita, dos dados pessoais é e continuará sendo realizada de acordo com as cláusulas relevantes da lei de proteção de dados aplicável (e, quando for o caso, foi notificada às autoridades relevantes do Estado membro onde o exportador de dados estiver estabelecido) e que não viole as cláusulas relevantes do Estado;

(b) que instrui e que, pela duração dos serviços de processamento de dados pessoais, irá instruir o importador de dados a processar os dados pessoais transferidos apenas em nome do exportador de dados e de acordo com a lei de proteção de dados aplicável e com as Cláusulas;

(c) que o importador de dados fornecerá garantias suficientes em relação às medidas de segurança organizacional e técnicas especificadas no Apêndice 2 deste contrato;

(d) que, após avaliação dos requisitos da lei de proteção de dados aplicável, as medidas de segurança sejam apropriadas para proteger os dados pessoais contra destruição acidental ou ilegal, ou perda acidental, alteração, revelação não autorizada ou acesso, principalmente quando o processamento envolver a transmissão de dados através de uma rede, e contra todas as outras formas ilegais de processamento, e que essas medidas garantam um nível de segurança apropriado aos riscos apresentados pelo processamento e que a natureza dos dados seja protegida em relação a sua qualidade e custo da implantação;

(e) que garantirá a conformidade com as medidas de segurança;

(f) que, se a transferência envolver categorias especiais de dados, o assunto dos dados seja informado de antemão, ou o mais rapidamente possível, de que seus dados podem estar sendo transmitidos a um país terceiro que não fornece proteção adequada dentro do significado da Diretriz 95/46/EC;

(g) encaminhar qualquer notificação recebida do importador de dados ou qualquer subprocessador em relação à Cláusula 5(b) e Cláusula 8(3) para a autoridade supervisora de proteção dos dados, se o exportador de dados decidir continuar a transferir ou retirar a suspensão;

(h) disponibilizar aos titulares dos dados, mediante solicitação, uma cópia das Cláusulas, com a exceção do Apêndice 2, e uma descrição resumida das medidas de segurança, além de uma cópia de qualquer contrato para serviços de subprocessamento, o que deve ser feito de acordo com as Cláusulas, a não ser que as Cláusulas ou o contrato contenham informações comerciais, em cujo caso tal informação comercial pode ser removida;

(i) que, no caso de subprocessamento, a atividade de processamento é realizada de acordo com a Cláusula 11 por um subprocessador fornecendo, no mínimo, o mesmo nível de proteção para os dados pessoais e os direitos do titular dos dados que o importador de dados diante das Cláusulas; e

(j) que irá garantir conformidade com a Cláusula 4(a) a (i).

Seção 5. Obrigações do importador de dados

O importador de dados concorda e garante:

(a) processar os dados pessoais apenas em nome do exportador de dados e em conformidade com suas instruções e com as Cláusulas; caso não possa fornecer essa conformidade por qualquer motivo, ele concorda em informar prontamente ao exportador de dados sobre sua incapacidade de conformidade, em cujo caso o exportador de dados terá o direito de suspender a transferência de dados e/ou rescindir o contrato;

(b) que não tem motivo para acreditar que a legislação aplicável impede que ele siga as instruções recebidas do exportador de dados e suas obrigações contratuais, e que no caso de uma mudança na legislação com chances de ter um efeito adverso substancial nas garantias e obrigações fornecidas pelas Cláusulas, ele irá notificar prontamente a mudança para o exportador de dados assim que tomar ciência, em cujo caso o exportador de dados terá o direito de suspender a transferência de dados e/ou rescindir o contrato;

(c) que implantou as medidas de segurança organizacionais e técnicas especificadas no Apêndice 2 antes de processar os dados pessoais transferidos;

(d) que irá notificar prontamente o exportador de dados sobre:

(i) qualquer solicitação vinculativa para revelação dos dados pessoais, por uma autoridade competente, salvo proibição de outra maneira, como uma proibição por lei criminal para preservar a confidencialidade de uma investigação oficial,
(ii) qualquer acesso acidental ou não autorizado, e
(iii) qualquer solicitação recebida diretamente dos titulares dos dados, sem responder a essa solicitação, a não ser que tenha sido autorizado de outra maneira;

(e) lidar de forma oportuna e adequada com todas as consultas do exportador de dados em relação ao processamento dos dados pessoais sujeitos à transferência, e seguir o conselho da autoridade supervisora em relação ao processamento dos dados transferidos;

(f) mediante solicitação do exportador de dados para submeter suas instalações de processamento de dados a uma auditoria das atividades de processamento cobertas pelas Cláusulas, que deve ser realizada pelo exportador de dados ou uma agência de inspeção composta por membros independentes e em posse das qualificações profissionais necessárias vinculadas por um dever de confidencialidade, selecionado pelo exportador de dados, quando aplicável, em acordo com a autoridade supervisora;

(g) tornar disponível ao titular dos dados, mediante solicitação, uma cópia das Cláusulas, ou qualquer contrato existente para subprocessamento, a não ser que as Cláusulas ou o contrato contenha informações comerciais, em cujo caso ele pode remover tal informação comercial, com a exceção do Apêndice 2, que deve ser substituído por uma descrição resumida das medidas de segurança nos casos em que o assunto dos dados não consiga obter uma cópia do exportador de dados;

(h) que, no caso de subprocessamento, tenha informado previamente ao exportador de dados e obtido seu consentimento prévio por escrito;

(i) que os serviços de processamento sejam realizados pelo subprocessador de acordo com a Cláusula 11;

(j) enviar prontamente uma cópia de qualquer acordo de subprocessador concluído sob as Cláusulas do exportador de dados.

Seção 6. Responsabilidade

1. As partes concordam que qualquer titular dos dados que tenha sofrido danos resultantes de qualquer brecha das obrigações mencionadas na Cláusula 3 ou na Cláusula 11, por qualquer parte ou subprocessador, tenha o direito de receber compensação do exportador de dados pelos danos sofridos.

2. Se um titular de dados não conseguir abrir uma reivindicação por compensação de acordo com o parágrafo 1 contra o exportador de dados, em decorrência de uma falha cometida pelo importador de dados ou seu subprocessador relativa a qualquer uma de suas obrigações mencionadas na Cláusula 3 ou na Cláusula 11, porque o exportador de dados tenha factualmente desaparecido ou deixado de existir perante a lei ou tenha falido, o importador de dados concorda que o assunto dos dados pode abrir uma reivindicação contra o importador de dados como se ele fosse o exportador de dados, a não ser que alguma entidade sucessora tenha assumido todas as obrigações legais do exportador de dados por contrato ou por força de lei, em cujo caso o titular dos dados pode reivindicar seus direitos contra essa entidade.

   O importador de dados não pode utilizar uma falha com as obrigações por parte de um subprocessador para evitar suas próprias responsabilidades.

3. Se um titular de dados não conseguir abrir uma reivindicação contra o exportador de dados ou importador de dados mencionados nos parágrafos 1 e 2, em decorrência de uma falha cometida pelo subprocessador relativa a qualquer uma de suas obrigações mencionadas na Cláusula 3 ou na Cláusula 11 porque o exportador de dados e o importador

de dados tenham factualmente desaparecido ou deixado de existir perante a lei ou tenham falido, o subprocessador concorda que o titular dos dados pode abrir uma reivindicação contra o subprocessador de dados em relação às suas próprias operações de processamento sob as Cláusulas, como se ele fosse o exportador de dados ou o importador de dados, a não ser que alguma entidade sucessora tenha assumido todas as obrigações legais do exportador de dados ou importador de dados por contrato ou por força de lei, em cujo caso o assunto dos dados pode reivindicar seus direitos contra essa entidade. A responsabilidade do subprocessador deve ser limitada a suas próprias operações de processamento diante das Cláusulas.

Seção 7. Mediação e jurisdição

1. O importador de dados concorda que, se o titular dos dados invocar contra si direitos beneficiários de terceiros e/ou reivindicar compensação por danos sob as Cláusulas, o importador de dados irá aceitar a decisão do titular dos dados:

   (a) de levar a disputa à mediação por uma pessoa independente ou, quando for o caso, pela autoridade supervisora;

   (b) de levar a disputa às cortes do Estado membro no qual o exportador de dados está estabelecido.

2. As partes concordam que a escolha feita pelo titular dos dados não irá prejudicar seus direitos substantivos ou de procedimento de buscar soluções de acordo com outras cláusulas de leis nacionais ou internacionais.

Seção 8. Cooperação com autoridades supervisoras

1. O exportador de dados concorda em depositar uma cópia deste contrato com a autoridade supervisora, caso ela assim solicite, ou se esse depósito for solicitado pela lei de proteção de dados aplicável.

2. As partes concordam que a autoridade supervisora tem o direito de conduzir uma auditoria do importador de dados, e de qualquer subprocessador, que tenha o mesmo escopo e esteja sujeito às mesmas condições que se aplicariam a uma auditoria do exportador de dados sob a lei de proteção de dados aplicável.

3. O importador de dados deve informar prontamente ao 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, em relação ao parágrafo 2. Nesse caso o exportador de dados deve ter o direito a tomar as medidas previstas na Cláusula 5 (b).

Seção 9. Lei vigente

As Cláusulas devem ser regidas pela lei do Estado Membro em que o exportador de dados esteja estabelecido.

Seção 10. Variação do contrato

As partes concordam em não variar nem modificar as Cláusulas. Isso não impossibilita as partes aditem cláusulas sobre questões relacionadas aos negócios, quando necessário, contanto que não contradigam a Cláusula.

Seção 11. Subprocessamento

1. O importador de dados não deve terceirizar nenhuma de suas operações de processamento realizadas em nome do exportador de dados sob as Cláusulas, sem o consentimento prévio por escrito do exportador de dados. Quando o importador de dados terceirizar suas obrigações diante das Cláusulas, com o consentimento o exportador de dados, ele deve fazê-lo apenas por meio de acordo escrito com o subprocessador, que impõe, sobre o subprocessador, as mesmas obrigações impostas sobre o importador de dados diante das Cláusulas. Quando o subprocessador não conseguir cumprir com suas obrigações de proteção dos dados diante de tal acordo por escrito, o importador de dados

deve permanecer totalmente responsável em relação ao exportador de dados pelo cumprimento das obrigações do subprocessador sob tal acordo.

2. O contrato prévio entre o importador de dados e o subprocessador também deve fornecer uma cláusula beneficiária a terceiro, conforme estabelecido na Cláusula 3, para casos em que o titular dos dados não conseguir abrir a reivindicação por compensação mencionada no parágrafo 1 da Cláusula 6 contra o exportador de dados ou importador de dados por eles terem desaparecido factualmente ou terem deixado de existir perante a lei ou tenham falido e no caso de nenhuma entidade sucessora ter assumido todas as obrigações legais do exportador de dados ou importador de dados por contrato ou força de lei. Essa responsabilidade de terceiros do subprocessador deve ser limitada a suas próprias operações de processamento diante das Cláusulas.

3. As cláusulas relativas a aspectos de proteção dos dados para subprocessamento do contrato mencionado no parágrafo 1 devem ser regidas pela lei do Estado Membro em que cada exportador estiver estabelecido.

4. O exportador de dados deve manter uma lista de acordos de subprocessamento concluídos sob as Cláusulas e deve ser notificado pelo importador de dados em relação à Cláusula 5 (j), que deve ser atualizada uma vez ao ano, no mínimo. A lista deve estar disponível à autoridade supervisora de proteção de dados do exportador de dados.

Seção 12. Obrigação após o encerramento dos serviços de processamento de dados pessoais

1. As partes concordam que, após o encerramento do fornecimento de serviços de processamento de dados, o importador de dados e o subprocessador devem, à escolha do exportador de dados, devolver todos os dados pessoais transferidos e as cópias desses dados ao exportador de dados, ou devem destruir todos os dados pessoais e certificar ao exportador de dados que assim o fizeram, a não ser que a legislação imposta ao importador de dados o impeça de devolver ou destruir todo ou parte dos dados pessoais transferidos. Nesse caso, o importador de dados irá garantir a confidencialidade dos dados pessoais transferidos e que não irá mais processar ativamente os dados pessoais transferidos.

2. O importador de dados e o subprocessador garantem que, mediante solicitação do exportador de dados e/ou da autoridade supervisora, irão submeter suas instalações de processamento de dados a uma auditoria das medidas mencionadas no parágrafo 1.

APÊNDICE 1 ÀS CLÁUSULAS CONTRATUAIS PADRÃO

Exportador de dados
O exportador de dados é (por favor especifique brevemente suas atividades relevantes para a transferência):

O Cliente é um assinante de um Serviço de nuvem fornecido pela SISW, que permite aos usuários finais autorizados pelo Cliente inserirem, modificarem, usarem, removerem, baixarem e processarem os Dados do Cliente, que podem incluir dados pessoais, conforme descrito no Acordo e na documentação relevante para o Serviço de nuvem.

Importador de dados
O importador de dados é (por favor especifique brevemente as atividades relevantes para a transferência):

A Siemens Product Lifecycle Management Software Inc., de forma independente e/ou por meio de seus subprocessadores, fornece o Serviço de nuvem, que inclui: manter infraestrutura de computação nos EUA e na UE sobre a qual o Serviço de nuvem é operado; armazenar na infraestrutura os Dados do cliente que forem transferidos para o Serviço de nuvem pelo Cliente; monitorar a disponibilidade e operação contínua do Serviço de nuvem e da infraestrutura; e manter a segurança da infraestrutura conforme estabelecido no Acordo e na documentação relevante para o Serviço de nuvem.

Titulares de dados
Os dados pessoais transferidos abrangem as seguintes categorias de titulares de dados (por favor especifique):

Salvo especificação expressa por escrito pelo exportador de dados, os titulares de dados podem incluir usuários finais autorizados pelo Cliente a utilizarem o Serviço de nuvem e outras pessoas do Cliente cujos dados pessoais estejam armazenados no Serviço de nuvem.

Categorias de dados
Os dados pessoais transferidos abrangem as seguintes categorias de dados (por favor especifique):

Categorias específicas de dados a serem armazenadas no Serviço de nuvem estão sujeitas à configuração significativa por parte do Cliente, embora algumas categorias comuns de dados que podem ser armazenadas no Serviço de nuvem incluem, mas não se limitam a: nome, endereço de e-mail, nome da empresa, número de telefone, local de trabalho, nacionalidade ou cidadania e informações relativas ao acesso e uso do Serviço de nuvem. Dependendo da configuração pelo Cliente do Serviço de nuvem, muitas outras categorias de dados podem estar presentes nos Dados do cliente.

Categorias especiais de dados (se for o caso)
Os dados pessoais transferidos abrangem as seguintes categorias especiais de dados (por favor especifique):

Quaisquer categorias especiais de dados a serem armazenadas no Serviço de nuvem seguem o acordado entre as partes no Acordo ou em um Pedido, ou conforme estabelecido em uma declaração de trabalho para serviços profissionais a serem fornecidos ao Cliente como parte da sua implantação do Serviço de nuvem.

Operações de processamento
Os dados pessoais transferidos estarão sujeitos às seguintes atividades de processamento básico (por favor especifique):

Os dados pessoais podem ser processados: como parte da operação normal do Serviço de nuvem, dependendo da configuração do Cliente; por meio de armazenamento e/ou arquivamento na infraestrutura de computação mantida pelo exportador de dados, em ambientes de um ou vários usuários; acessados ou transmitidos de acordo com as instruções enviadas ao Serviço de nuvem por um usuário final autorizado pelo Cliente a usar o Serviço de nuvem; e como parte das operações de manutenção do Serviço de nuvem realizadas pelo exportador de dados.

APÊNDICE 2 ÀS CLÁUSULAS CONTRATUAIS PADRÃO

Algumas ofertas de Serviços de nuvem são fornecidas sob diferentes termos, o que, se for o caso, será estabelecido em um Pedido. Do contrário, o importador de dados tomará as medidas organizacionais e técnicas descritas abaixo, em respeito aos dados pessoais armazenados no Sistema, de acordo com as Cláusulas 4(d) e 5(c) das Cláusulas.

Descrição das medidas de segurança organizacionais e técnicas implantadas pelo importador de dados, de acordo com as Cláusulas 4(d) e 5(c):

1. Controle de acesso físico. Pessoas não autorizadas não terão acesso físico às instalações, prédios ou salas onde estiverem localizados os sistemas de processamento de dados que processam e/ou utilizam os dados pessoais.

   Medidas: Todos os centros de dados seguem procedimentos rigorosos de segurança que são garantidos por pessoal de segurança, equipamento de vigilância, detectores de movimento, mecanismos de controle de acesso e outras medidas para evitar que as instalações do equipamento e centros de dados sejam comprometidos. Apenas representantes autorizados têm acesso a sistemas e infraestrutura dentro das instalações de centros de dados. Para garantir funcionalidade adequada, os equipamentos de segurança física (por exemplo, sensores de movimento, câmeras, etc.) passam regularmente por manutenção. Em maiores detalhes, as seguintes medidas de segurança física são implantadas em todos os centros de dados:

   a. Em geral, os prédios são protegidos por sistemas de controle de acesso (sistema de acesso através de cartão inteligente).
   b. Credenciais de autorização, que incluem um crachá eletrônico de acesso (exclusivo do funcionário, fornecedor ou terceirizado) e PIN, são fornecidos ao pessoal autorizado para o aceso físico às instalações do centro de dados.
   c. O acesso físico aos centros de dados dentro dos limites do sistema é controlado por um sistema eletrônico de controle de acesso, que compreende leitores de cartão e teclados de PIN para entrada em prédios e salas, e apenas leitores de cartão para a saída de prédios e salas.
   d. Dependendo da classificação de segurança, prédios, áreas destacadas e o entorno dos terrenos são protegidos também por medidas adicionais. Elas incluem perfis de acesso específicos, vigilância por vídeo, sistemas de alarme contra invasores e sistemas de controle de acesso por biometria.
   e. Os direitos de acesso serão dados a pessoas autorizadas, de forma individual, de acordo com as medidas de Controle de acesso aos dados e sistema definidas abaixo. Isso também se aplica ao acesso de visitantes. Convidados e visitantes nos prédios da SISW devem cadastrar seus nomes na recepção e precisam ser acompanhados por pessoal autorizado da SISW. A SISW e todos os fornecedores de centro de dados terceirizados registram os nomes e horários em que as pessoas entram nas áreas privativas da SISW dentro dos centros de dados.
   f. Os funcionários da SISW e o pessoal externo precisam usar seus crachás em todos os locais da SISW.

2. Controle de acesso ao sistema. Deve haver uma prevenção ao uso não autorizado dos sistemas de processamento de dados.

   Medidas:

   a. A SISW ou seus subprocessadores gerenciam o ambiente de acordo com o Controle de Acesso NIST SP 800-53 Rev 4 (AC) e requisitos de Identificação e autenticação (IA).
   b. Diversos níveis de autorização são utilizados para dar acesso a sistemas sensíveis, incluindo os que armazenam e processam os dados pessoais. Os processos são estabelecidos para garantir que apenas os usuários autorizados tenham a autorização adequada para adicionar, excluir ou modificar usuários.
   c. Todos os usuários acessam os sistemas da SISW com um nome de usuário e senha únicos, e essas credenciais precisam atender a determinados critérios de complexidade.
   d. A SISW e seus subprocessadores têm procedimentos estabelecidos para garantir que as mudanças de autorização solicitadas sejam implantadas apenas de acordo com as diretrizes (por exemplo, nenhum direito deve ser fornecido sem autorização). Se um usuário da SISW mudar de cargo ou sair da empresa, um processo é aberto para revogar os direitos de acesso ao ambiente.
   e. A SISW e os subprocessadores estabeleceram uma política que proíbe o compartilhamento de senhas, determina o que fazer no caso de uma senha ser revelada, exige trocas regulares de senha e também que as senhas padrão sejam alteradas. IDs de usuário personalizadas são designadas para autenticação. Todas as senhas devem atender a requisitos mínimos de complexidade e devem ser armazenadas de maneira criptografada. No caso de senhas de domínio, o sistema força uma alteração a cada 60 dias e essa senha precisa atender a requisitos mínimos de complexidade. Cada computador da SISW tem uma proteção de tela protegida por senha.
   f. A SISW ou seus subprocessadores fazem uma auditoria automática dos seguintes eventos de conta: criação, alteração, ativação, desativação e remoção. Um administrador de sistema revisa os registros periodicamente.

g. As redes da SISW e de seus subprocessadores são protegidas da Internet publica por firewalls.
h. A SISW e seus subprocessadores utilizam software antivírus atualizado nos pontos de acesso à rede da empresa para contas de e-mail, e em todos os servidores de arquivo e estações de trabalho.
i. A SISW e seus subprocessadores implantam gerenciamento de reparo de segurança para garantir a implantação de atualizações relevantes de segurança.
j. O acesso remoto completo à rede corporativa da SISW e a infraestrutura crítica é protegida por autenticação forte de diversos fatores.

3. Controle de acesso aos dados. O pessoal com direito a usar os sistemas de processamento de dados ganharão acesso apenas aos dados pessoais a que têm direito a acessar, e os dados pessoais não devem ser lidos, copiados, modificados nem removidos sem autorização durante o processamento, uso e armazenamento.

   Medidas:
   a. O acesso a informações pessoais, confidenciais ou sensíveis é garantido de acordo com a necessidade. Em outras palavras, os funcionários ou terceiros externos têm acesso às informações de que precisam para realizar seu trabalho. A SISW usa conceitos de autorização que documentam como as autorizações são atribuídas e quais autorizações são atribuídas. Todos os dados pessoais, confidenciais ou sensíveis de alguma outra maneira são protegidos de acordo com as normas e políticas de segurança da SISW.
   b. Todos os servidores de produção de qualquer Serviço de nuvem da SISW são operados nos centros de dados relevantes. As medidas de segurança que protegem aplicativos que processam informações pessoais, confidenciais ou outras informações sensíveis são verificadas regularmente. Com esse propósito, a SISW também incorpora auditorias periódicas para confirmar que essas medidas sejam aplicadas de maneira adequada.
   c. A SISW não permite a instalação de software pessoal ou qualquer outro software não aprovado pela SISW nos sistemas utilizados para qualquer Serviço de nuvem.
   d. Caso haja a necessidade de transferir dados por conta de uma falha da mídia de armazenamento de dados subjacente, após a conclusão da transferência, a mídia de armazenamento defeituosa será desmagnetizada (no caso de armazenamento magnético) ou destruída (no caso de armazenamento óptico ou em estado sólido).

4. Controle de transmissão dos dados. Os dados pessoais não devem ser lidos, copiados, modificados nem removidos sem autorização durante a transferência.

   Medidas:
   a. A SISW ou seu subprocessador irá gerenciar a infraestrutura e a configuração para atender aos requisitos da Proteção de comunicação e sistemas NIST SP 800-53 Rev 4 (SC). Isso inclui sistemas de prevenção contra invasão baseada na rede (NIPS) e firewalls nos limites do sistema para proteger contra comunicações mal-intencionadas no limite externo da infraestrutura. Os NIPS e firewalls são configurados de acordo com as normas DISA STIG. Os dados são criptografados em trânsito usando módulos criptográficos de acordo com FIPS 140-2.
   b. Nos casos em que os portadores de dados são fisicamente transportados, medidas adequadas são implantadas na SISW para garantir os níveis de serviço acordados (por exemplo, criptografia e recipientes revestidos com chumbo).
   c. A transmissão dos dados pessoais por meio de redes SISW internas é protegida da mesma forma que muitos outros dados confidenciais, de acordo com as políticas de segurança da SISW.
   d. Quando os dados forem transferidos entre a SISW e o Cliente, as medidas de proteção para os dados pessoais transferidos são as estabelecidas no Acordo ou na documentação relevante para o Serviço de nuvem. Isso se aplica à transferência baseada em rede e física de dados. O cliente assume a responsabilidade por todas as transferências de dados a partir do Ponto de demarcação da SISW (por exemplo, firewall de saída do data center que hospeda o Serviço de nuvem).

5. Controle de entrada dos dados. O Serviço de nuvem permitirá determinação retrospectiva se e por quem os dados pessoais tiverem sido inseridos, modificados ou removidos da infraestrutura utilizada para fornecer o Serviço de nuvem.

   Medidas:
   a. A SISW permite que apenas o pessoal autorizado acesse os dados pessoais, conforme necessário no curso do trabalho. A SISW implantou um sistema de registro para entrada, modificação e exclusão ou bloqueio de dados pessoais pela SISW ou seus subprocessadores, até o máximo suportado pelo Serviço de nuvem.
   b. As trilhas de auditoria fornecem o detalhe suficiente necessário para facilitar a reconstrução dos eventos, caso exista uma suspeita ou confirmação de atividade não autorizada ou mau funcionamento. Cada registro de evento

do sistema operacional inclui o tipo de evento, marcação de data/hora, a fonte do evento, o local do evento, o resultado do evento e o usuário associado ao evento.

6. Controle de trabalho. Os dados pessoais serão processados exclusivamente de acordo com os temos do Acordo e quaisquer instruções relacionadas fornecidas pelo Cliente.

   Medidas:
   a. A SISW usa controles e processos para garantir a conformidade com contratos entre a SISW e seus clientes, subprocessadores ou outros prestadores de serviço.
   b. Os Dados do cliente estarão sujeitos a, no mínimo, o mesmo nível de proteção das informações confidenciais, de acordo com a norma de Classificação da informação da SISW.
   c. Todos os funcionários da SISW e parceiros de contrato são vinculados contratualmente para respeitar a confidencialidade de todas as informações sensíveis, incluindo segredos comerciais dos parceiros e clientes da SISW.

7. Controle de disponibilidade. Os dados pessoais serão protegidos contra perda ou destruição não autorizada ou acidental.

   Medidas:
   a. A SISW emprega os processos de backup e outras medidas que garantem rápida restauração dos sistemas críticos de negócios, como e quando necessário.
   b. A SISW confia em prestadores de serviço globais de nuvem para garantir disponibilidade para os centros de dados.
   c. A SISW definiu planos de contingência e estratégias de recuperação de desastres e dos negócios para Serviços de nuvem.

8. Controle de separação dos dados. Os dados pessoais coletados para diferentes propósitos podem ser processados em separado.

   Medidas:
   a. Quando aplicável, a SISW usa as capacidades técnicas do software implantado (por exemplo: cenários de sistema separado ou de diversos usuários) para alcançar a separação de dados entre os dados pessoais do Cliente e os dos outros clientes.
   b. A SISW mantém instâncias dedicadas (com separação lógica ou física) para cada cliente.
   c. O Cliente (incluindo suas Afiliadas) tem acesso apenas a suas próprias instâncias de cliente.

9. Controle de integridade dos dados. Garante que os dados pessoais permanecerão intactos, completos e atuais durante as atividades de processamento:

   Medidas: A SISW implantou uma estratégia de defesa em diversas camadas como uma proteção contra modificações não autorizadas. Isso se refere a controles, conforme declarado nas seções de medidas e controles descritas acima. A configuração de firewalls resultará em diversos segmentos de rede que separam os acessos público e privado. Cada regra de firewall estabelecida terá controles de acesso específicos definindo as comunicações permitidas entre esses segmentos.

   a. Central de monitoração de segurança: Software de detecção de invasão automatizado será usado em conjunto com outros processos e softwares forenses e de prevenção de segurança para alertar, investigar e, se necessário, notificar e auxiliar na solução de qualquer incidente de segurança.
   b. Software antivírus: todos os sistemas terão as definições de antivírus atuais configuradas para proteger contra vírus, worms, trojans e outras formas de malware.
   c. Backup e recuperação: todos os sistemas terão um nível básico de instantâneos de backup dos dados e configurações. Se for o caso, a SISW e seus subprocessadores também operarão uma instância do cliente, com configuração de alta disponibilidade, que garantirá que os dados sejam armazenados em dois centros de dados separados, com distância suficiente entre si.
   d. Auditorias externas regulares para comprovar as medidas de segurança. A SISW e seus subprocessadores passarão por auditorias externas periódicas para testar as medidas de segurança listadas acima.