

ÚLTIMA ATUALIZAÇÃO: 22 de junho de 2021

Adendo sobre o Processamento de Dados

Este Adendo sobre o Processamento de Dados (o "DPA") é um adendo ao Contrato de Licença de Usuário Final da Lincoln Electric Company ("EULA") e é aplicável entre a Lincoln Electric Company (o "Processador de Dados") e o Usuário Autorizado de acordo com o EULA (o "Controlador de Dados"), (cada um deles uma "Parte" e, juntos, as "Partes").

CONSIDERANDO QUE

O EULA rege o direito do Usuário Autorizado de usar o Aplicativo Licenciado e, conforme aplicável, outros serviços online fornecidos pela Lincoln Electric Company. Para fins de cumprimento de suas obrigações sob o EULA, a Lincoln Electric Company atuará como um Processador de Dados em nome do Usuário Autorizado. A fim de garantir a conformidade com as regulamentações de Dados Pessoais, as Partes concordaram em complementar o EULA para estabelecer os termos e condições aplicáveis ao Processamento de Dados Pessoais pelo Processador de Dados em nome do Controlador de Dados.

FICA ACORDADO QUE

1. DEFINIÇÕES

1.1 Neste DPA, os termos em maiúsculas devem ter os seguintes significados, a menos que definidos no EULA ou de qualquer outra forma de acordo com o contexto:

"Controlador de Dados"	significa a entidade que determina as finalidades e meios do Processamento de Dados Pessoais;
"Processador de Dados"	significa a entidade que processa Dados Pessoais em nome do Controlador de Dados;
"Titular dos Dados"	significa um indivíduo identificado ou identificável, cujos Dados Pessoais estejam sendo processados;
"Instruções"	significa as instruções fornecidas pelo Controlador de Dados ao Processador de Dados para Processar Dados Pessoais de acordo com a prestação de serviços contida no EULA;
"Dados Pessoais"	significa qualquer informação relacionada a um indivíduo identificado ou identificável; um indivíduo identificável é aquele que pode ser identificado, direta ou indiretamente, particularmente por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos de sua identidade física, fisiológica, genética, mental, econômica, cultural ou social;
"Violação de dados pessoais"	significa uma violação de segurança que leva à destruição, perda, alteração, divulgação não autorizada de, ou acesso, acidental ou ilegal, a Dados Pessoais transmitidos, armazenados ou processados de qualquer outra forma ;
"Processo" /"Processamento" /"Processado"	significa qualquer ação realizada em Dados Pessoais, como coleta, registro, organização, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação, transferência ou disponibilização de qualquer outra forma, alinhamento ou combinação, restrição, exclusão ou destruição;
"Serviços de Processamento"	significa o Processamento de Dados Pessoais pelo Processador de Dados em conexão com o EULA;
"Categorias especiais de Dados pessoais"	significa quaisquer Dados Pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação em sindicatos, associações ou fundações, aparência, processos penais e medidas de segurança, informações financeiras e de propriedade, informações de paradeiro ou informações de crédito, e o Processamento de dados genéticos, dados biométricos para fins de identificação única de uma pessoa natural, dados relativos à saúde ou dados relativos à vida

sexual ou orientação sexual de uma pessoa natural, ou dados relativos a menores de idade com 14 anos ou menos;

“Cláusulas Contratuais Padrão”

significa as cláusulas contratuais padrão adotadas pela Decisão da Comissão da UE 2010/87, de 5 de fevereiro de 2010, sobre cláusulas contratuais padrão para a transferência de dados pessoais para processadores estabelecidos em países terceiros ou qualquer conjunto substituto de cláusulas padrão acordadas entre as Partes. Quando o Controlador de Dados estiver estabelecido em uma jurisdição fora da União Europeia, as referências aos Estados Membros nas disposições substantivas das Cláusulas Contratuais Padrão devem ser interpretadas como referências à jurisdição onde o Controlador de Dados está estabelecido;

“Subprocessador”

significa qualquer processador contratado pelo Processador de Dados (ou por qualquer outro Subprocessador do Processador de Dados) para Processar Dados Pessoais em nome do Controlador de Dados de acordo com suas Instruções e com os termos do subcontrato por escrito.

1.2 As legendas e cabeçalhos de seção usados são apenas para fins de referência e conveniência, e não fazem parte deste DPA e não devem ser usados na interpretação deste DPA.

2. ESCOPO E APLICAÇÃO DESTE DPA

2.1 Este DPA apenas complementa as disposições do EULA em relação aos Serviços de Processamento fornecidos pelo Processador de Dados ao Controlador de Dados, de acordo com o EULA.

3. PROCESSAMENTO DE DADOS

3.1 O Processador de Dados concorda em Processar os Dados Pessoais de acordo com os termos e condições estabelecidos neste DPA e, em particular, o Processador de Dados compromete-se:

3.1.1 a processar os Dados Pessoais apenas em nome do Controlador de Dados e sempre em conformidade com as Instruções do Controlador de Dados, conforme definido neste DPA, e com todas as leis de proteção de dados aplicáveis;

3.1.2 a garantir que qualquer funcionário encarregado dos Serviços de Processamento se comprometa com a confidencialidade ou esteja sob uma obrigação legal e apropriada de confidencialidade;

3.1.3 a tomar medidas técnicas, físicas e organizacionais para garantir a segurança e confidencialidade dos Dados Pessoais e proteger adequadamente os Dados Pessoais Processados em nome do Controlador de Dados contra uso indevido e perda, conforme previsto no Anexo 2 deste DPA;

3.1.4 que notificará imediatamente o Controlador de Dados sobre: (a) qualquer solicitação legalmente vinculativa de divulgação de Dados Pessoais por uma autoridade governamental, a menos que seja proibido de outra forma, como uma proibição sob a lei criminal de preservar a confidencialidade de uma aplicação da lei ou investigação de inteligência, (b) qualquer Violação de Dados Pessoais que afete os Dados Pessoais processados em nome do Controlador de Dados, (c) qualquer solicitação recebida diretamente dos Titulares dos Dados (incluindo direitos de acesso, retificação, exclusão, objeção, restrição, transferência de dados e o direito de não estar sujeito a uma decisão baseada exclusivamente no Processamento automatizado, incluindo criação de perfil); o Processador de Dados (i) não responderá diretamente a essa solicitação, exceto para notificar o Titular dos Dados que está agindo em nome do Controlador de Dados, e para fornecer ao Titular dos Dados as informações de contato do Controlador de Dados, e (ii) levando em conta a natureza do Processamento, auxiliará o Controlador dos Dados nas medidas técnicas, físicas e organizacionais adequadas, na medida do possível, para o cumprimento da obrigação do Controlador dos Dados de responder às solicitações de exercício dos direitos do Titular dos Dados;

3.1.5 fornecer cooperação comercialmente razoável ao Controlador de Dados para auxiliar o Controlador de Dados a cumprir suas próprias obrigações legais relacionadas à segurança dos Dados Pessoais, tais

como: notificação de uma Violação de Dados Pessoais à autoridade supervisora competente, comunicação de tal Violação de Dados Pessoais aos Titulares dos Dados afetados e, quando aplicável, implementação de avaliações de impacto na proteção de dados e consultas prévias às autoridades de supervisão, levando em conta a natureza do Processamento e a informação à disposição do Processador de Dados;

- 3.1.6 disponibilizar ao Controlador de Dados todas as informações necessárias para comprovar o cumprimento das obrigações estabelecidas neste DPA e permitir e contribuir para auditorias, incluindo inspeções, conduzidas pelo Controlador de Dados ou outro auditor determinado pelo Controlador de Dados, conforme estabelecido na Seção 6; e,
- 3.1.7 que quaisquer Serviços de Processamento realizados por um Subprocessador serão realizados de acordo com a Seção 7.

3.2 No que diz respeito aos Serviços de Processamento, o Controlador de Dados será responsável por cumprir todas as exigências que se aplicam a ele sob a legislação aplicável em relação ao Processamento de Dados Pessoais e as Instruções emitidas para o Processador de Dados. Particularmente, mas sem prejuízo da generalidade do que foi mencionado anteriormente, o Controlador de Dados reconhece e concorda que será o único responsável pelo seguinte: (i) a exatidão, qualidade e legalidade dos Dados Pessoais; (ii) cumprir todas as exigências de transparência e legalidade necessárias sob a lei aplicável para a coleta e uso dos Dados Pessoais, incluindo a obtenção de quaisquer consentimentos e autorizações necessários dos Titulares dos Dados ou de qualquer outra forma; (iii) garantir que o Controlador de Dados tenha o direito de transferir ou fornecer acesso aos Dados Pessoais para o Processador de Dados e que o Controlador de Dados tenha fornecido todas as notificações necessárias e obtido todos os consentimentos e/ou autorizações necessários em relação a essa transferência ou acesso e, de forma mais geral, para Processamento de acordo com os termos do EULA (incluindo este DPA); e (iv) assegurar que suas Instruções cumpram as leis aplicáveis. Mediante solicitação do Processador de Dados, o Controlador de Dados fornecerá ao Processador de Dados, em até três (3) dias úteis, evidências por escrito de tais notificações, consentimentos e autorizações. O Controlador de Dados não inserirá nos Serviços de Processamento, ou de qualquer outra forma fornecerá ao Processador de Dados quaisquer Categorias Especiais de Dados Pessoais, a menos que de outra forma acordado separadamente por escrito pelo Controlador de Dados. O Controlador de Dados informará o Processador de Dados, imediatamente e sem atrasos indevidos, se o Controlador de Dados não for capaz de cumprir suas responsabilidades estabelecidas neste DPA. O Usuário Autorizado é o único responsável por revisar os Serviços de Processamento, incluindo qualquer documentação e recursos de segurança disponíveis, para determinar se eles atendem as exigências, necessidades comerciais e obrigações legais do Usuário Autorizado.

3.3 O Controlador de Dados autoriza o Processador de Dados a tornar anônimos os Dados Pessoais Processados, de acordo com o EULA, para obter dados analíticos relacionados ao uso do Aplicativo Licenciado e dos produtos e equipamentos Lincoln. O uso extra dos dados estatísticos resultantes pelo Processador de Dados não está sujeito a autorização prévia do Controlador de Dados.

4. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

4.1 O Controlador de Dados reconhece e concorda que, para fornecer os Serviços de Processamento sob o EULA, o Processador de Dados pode transferir e reter Dados Pessoais nos Estados Unidos da América e em qualquer outro país onde o Processador de Dados esteja localizado, para fins de fornecimento dos Serviços de Processamento. Portanto, no decorrer da prestação dos Serviços de Processamento, pode ser necessário transferir Dados Pessoais para o Processador de Dados localizado fora do país de estabelecimento do Controlador de Dados. Se o Controlador de Dados estiver localizado no Espaço Econômico Europeu ou na Suíça, as Partes se comprometem a aplicar as disposições das Cláusulas Contratuais Padrão para a transferência de Dados Pessoais pelo Controlador de Dados (atuando como exportador de dados, de acordo com as Cláusulas Contratuais Padrão) para o Processador de Dados (atuando como importador de dados, de acordo com as Cláusulas Contratuais Padrão).

4.2 Se o Controlador de Dados estiver localizado fora do Espaço Econômico Europeu e da Suíça, as Partes também se comprometem a aplicar as disposições das Cláusulas Contratuais Padrão para a transferência de Dados Pessoais pelo Controlador de Dados (atuando como exportador de dados, de acordo com as Cláusulas Contratuais Padrão) para o Processador de Dados (atuando como importador de dados, de acordo com as Cláusulas Contratuais Padrão), desde que as Cláusulas Contratuais Padrão sejam legalmente exigidas e

suficientes para atender as exigências das regulamentações de proteção de dados aplicáveis para a transferência de Dados Pessoais pelo Controlador de Dados para o Processador de Dados, de acordo com o EULA.

4.3 Se as Partes aplicarem as Cláusulas Contratuais Padrão de acordo com as Seções 4.1 ou 4.2 deste DPA:

4.3.1 O Apêndice 1 das Cláusulas Contratuais Padrão deve ser aplicado da seguinte forma: (a) Exportador de dados: o Controlador de Dados, (b) Importador de dados: o Processador de Dados, (c) Titulares dos dados: pessoal do Controlador de Dados (o Usuário Autorizado), (d) Categorias de dados: dados relacionados ao uso de produtos e equipamentos de propriedade, licenciados ou gerenciados pelo Processador de Dados, conforme monitorado pelo Aplicativo Licenciado, de acordo com o EULA, incluindo dados de registro (ou seja, nomes de usuário e senhas), (e) Categorias especiais de dados pessoais: N/D, e (f) Operações de processamento: coleta, cópia, transferência, armazenamento, modificação, exclusão e outras operações necessárias para os Serviços de Processamento, de acordo com o EULA.

4.3.2 A descrição das medidas de segurança técnicas, físicas e organizacionais implementadas pelo Processador de Dados, atuando como importador de dados para os fins do Apêndice 2 das Cláusulas Contratuais Padrão, deve acontecer conforme previsto no Anexo 2 deste DPA.

4.4 Se as Cláusulas Contratuais Padrão forem aplicáveis entre as Partes, de acordo com a Seção 4.1 ou 4.2, suas disposições serão consideradas incorporadas a este DPA por referência, a menos que as Partes executem as Cláusulas Contratuais Padrão como um documento separado, de acordo com a Seção 4.5.

4.5 Na medida exigida pelas regulamentações de proteção de dados aplicáveis, as Partes devem celebrar e executar as Cláusulas Contratuais Padrão como um documento separado.

5. RESCISÃO

5.1 Este DPA entrará em vigor na data de vigência do EULA.

5.2 Este DPA deixará de existir automaticamente após a rescisão ou expiração (a) do EULA ou (b) das obrigações do Processador de Dados em relação aos Serviços de Processamento, e tal rescisão não exigirá uma ordem judicial ou procedimento judicial ou qualquer outra ação do Processador de Dados, do Controlador de Dados ou de qualquer outra parte para ter efeito. Quando aplicável, no término deste DPA, o Processador de Dados deve devolver ao Controlador de Dados ou excluir, a pedido do Controlador de Dados, todos os Dados Pessoais do Controlador de Dados em sua posse ou sob seu controle. Mediante solicitação do Controlador de Dados, o Processador de Dados deve confirmar o cumprimento de tais obrigações por escrito e excluir todas as cópias existentes, a menos que a lei aplicável exija o armazenamento ou permita a retenção dos Dados Pessoais.

5.3 O Controlador de Dados terá o direito de rescindir este DPA através de notificação por escrito ao Processador de Dados se o Processador de Dados estiver violando material ou persistentemente este DPA e, no caso de uma violação passível de reparação, não ter sido corrigida dentro de trinta (30) dias úteis a partir da data de recebimento pelo Processador de Dados de um aviso do Controlador de Dados identificando a violação e exigindo sua reparação.

5.4 O Processador de Dados terá o direito de rescindir este DPA por meio de notificação por escrito ao Controlador de Dados se o Controlador de Dados estiver violando material ou persistentemente este DPA e, no caso de uma violação passível de reparação, não ter sido corrigida dentro de trinta (30) dias úteis a partir da data de recebimento pelo Controlador de Dados de uma notificação do Processador de Dados identificando a violação e exigindo sua reparação.

6. AUDITORIAS E SOLICITAÇÕES DE INFORMAÇÃO

6.1 Dentro do limite de 1 (uma) auditoria por ano e sujeito à notificação do Controlador de Dados com 30 (trinta) dias de antecedência, exceto no caso de uma auditoria solicitada por uma autoridade supervisora, o Controlador de Dados pode, durante o horário comercial normal, sem interferir injustificadamente nas operações comerciais do Processador de Dados, auditar pessoalmente o Processador de Dados ou nomear um auditor terceirizado, sujeito às obrigações de confidencialidade para realizar tal auditoria.

6.2. O Processador de Dados deve cooperar no caso de uma auditoria nos termos desta Seção 6 e fornecer ao Controlador de Dados todas as informações necessárias para que tal auditoria seja realizada. O Controlador de Dados deve cobrir os custos e despesas incorridos por cada uma das partes em relação às auditorias nos termos desta Seção 6.

7. NOMEAÇÃO DE SUBPROCESSADORES

7.1 O Controlador de Dados autoriza o Processador de Dados a usar o serviço de Subprocessadores, listados na página acessível no endereço [<https://www.lincolnelectric.com/en/Legal-Information/Subprocessors>], somente conforme necessário para a prestação dos Serviços em conexão com o EULA.

7.2 O Controlador de Dados autoriza o Processador de Dados a usar os serviços de novos Subprocessadores, sujeito a notificação prévia ao Controlador de Dados pelo Processador de Dados com 15 (quinze) dias de antecedência face a mudança do Subprocessador. Se o Controlador de Dados tiver objeções à mudança do Subprocessador notificado, o Controlador de Dados pode, durante o período de notificação, rescindir este DPA por escrito. Se o Controlador de Dados não rescindir dentro do período da notificação, isso formaliza o consentimento do Controlador de Dados para a mudança notificada de Subprocessador.

7.3 Em qualquer caso, quando o Processador de Dados usa os serviços de um Subprocessador, este último será, por meio de contrato, obrigado a obedecer as mesmas obrigações às quais o Processador de Dados está vinculado em termos de Processamento de Dados Pessoais, nos termos deste DPA.

8. DISPOSIÇÕES DIVERSAS

8.1 Emendas ou aditivos a este DPA devem ser feitos por escrito para se tornarem efetivos. Não obstante o acima exposto, o Processador de Dados pode, a qualquer momento e sem aviso prévio ao Controlador de Dados, alterar as medidas técnicas, físicas e organizacionais estabelecidas no Anexo 2, desde que tais alterações não afetem materialmente a segurança, confidencialidade ou integridade dos Dados Pessoais.

8.2 As referências neste DPA sobre “por escrito” ou “escrito” incluem comunicações por e-mail e correio certificado.

8.3 Caso qualquer disposição deste DPA seja ou se torne inválida, isso não afetará a validade dos termos restantes. No caso de invalidação de qualquer disposição deste DPA, as Partes deverão, em qualquer caso, procurar, de boa fé, substituir a disposição invalidada por outra, exequível, válida e legal, tendo na maior medida possível um impacto jurídico igual ou equivalente ao da provisão inicial.

8.4 Este DPA é regido pela mesma lei que o EULA.

ANEXO 1 - TERMOS ESPECÍFICOS DA JURISDIÇÃO

Quando o Controlador de Dados está estabelecido em uma das jurisdições listadas neste Anexo 1, os seguintes termos se aplicam ao DPA, e tais termos devem substituir e serem dominantes no caso de qualquer conflito com as outras disposições do DPA. Todos os termos do EULA que não são especificamente modificados pelos termos específicos da jurisdição aplicável neste Anexo permanecem inalterados e em pleno vigor e efeito.

Brasil:

As Partes reconhecem e concordam que a seguinte alteração ao DPA deve ser aplicada:

- a) Todas as ocorrências de “Categorias especiais de dados pessoais” no DPA serão substituídas por “Dados pessoais confidenciais”.

México:

As Partes reconhecem e concordam que as seguintes alterações ao DPA devem ser aplicadas:

- a) Todas as ocorrências de “Categorias especiais de dados pessoais” no DPA serão substituídas por “Dados pessoais confidenciais”;
- b) Para a aplicação das Cláusulas Contratuais Padrão, todas as referências a “transferências” de dados pessoais devem ser interpretadas como remissões de dados pessoais, de acordo com a Lei Federal Mexicana sobre a Proteção de Dados Pessoais mantidos por Partes Privadas (“*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*”).

Rússia:

Além das disposições do DPA, as Partes comprometem-se com o seguinte:

- a) O Processador de Dados confirma aqui que está totalmente ciente de que o objetivo das atividades de Processamento de Dados Pessoais, de acordo com o DPA, é apenas fornecer os Serviços de Processamento e deve processar os Dados Pessoais apenas para a finalidade para a qual os Dados Pessoais são divulgados e aqueles que o Controlador de Dados exige do Processador de Dados. Além disso, o Processador de Dados deve confirmar prontamente por escrito que esta regra é observada mediante solicitação do Controlador de Dados.
- b) Antes de divulgar os Dados Pessoais originados de cidadãos russos ao Processador de Dados, o Controlador de Dados deve garantir que todos esses Dados Pessoais tenham sido registrados, sistematizados, acumulados, armazenados, esclarecidos (atualizados, alterados) e extraídos com o uso de bancos de dados localizados no território da Federação Russa, quando tais Dados Pessoais forem coletados de qualquer maneira, inclusive por meio da Internet.
- c) Se o Controlador de Dados detectar processamento ilegal ou imprecisão dos Dados Pessoais, o Controlador de Dados deverá instruir imediatamente o Processador de Dados a bloquear esses Dados Pessoais e iniciar uma inspeção. Os Dados Pessoais afetados serão bloqueados durante todo o período de inspeção. Se a inspeção confirmar a inexistência dos Dados Pessoais, o Controlador de Dados deve solicitar ao Titular dos Dados (seu representante) ou à autoridade de proteção de dados (se aplicável) as alterações e encaminhá-las ao Processador de Dados. Dados pessoais imprecisos devem ser alterados o quanto antes e dentro de sete (7) dias úteis, no máximo, a partir do dia em que as alterações foram entregues ao Processador de Dados. Os Dados Pessoais serão desbloqueados imediatamente após a alteração.
- d) Se for detectado que os Dados Pessoais são processados ilegalmente, o Controlador de Dados instruirá o Processador de Dados a interromper esse processamento ilegal dentro de três (3) dias úteis a partir da data da detecção. Se parecer ser impossível eliminar as violações e garantir a legalidade do processamento de Dados Pessoais, o Controlador de Dados instruirá o Processador de Dados a destruir os Dados Pessoais processados ilegalmente no prazo de dez (10) dias úteis a partir da data da detecção. O Controlador de Dados também é obrigado a notificar o Titular dos Dados (seu representante) e, quando exigido por lei, a autoridade de proteção de dados sobre a eliminação das violações.
- e) Se um Titular dos Dados revogar seu consentimento para o processamento de Dados Pessoais, o Controlador de Dados notificará imediatamente o Processador de Dados e o Processador de Dados interromperá o processamento e destruirá os Dados Pessoais deste Titular de Dados no prazo de trinta (30) dias a partir da data do recebimento do aviso de cancelamento pelo Controlador de Dados.
- f) Se for impossível cumprir os prazos estabelecidos nas Cláusulas d) e e) acima, o Processador de Dados bloqueará os Dados Pessoais relevantes a pedido do Controlador de Dados por no máximo seis (6) meses e destruirá esses Dados Pessoais dentro do mesmo período, a menos que a lei aplicável prescreva o contrário.

África do Sul:

As Partes reconhecem e concordam que as seguintes alterações ao DPA devem ser aplicadas no que diz respeito às definições fornecidas na seção 1 do DPA:

- a) “Titular dos Dados” significa uma pessoa cujos Dados Pessoais estão sendo processados.
- b) “Dados pessoais” significam informações pessoais, conforme definido na POPIA, incluindo quaisquer informações relacionadas a um indivíduo identificado ou identificável.
- c) “POPIA” é a Lei de Proteção de Informações Pessoais da África do Sul, a Lei 4 de 2013, e qualquer regulamentação, diretiva, decisão, ordem ou diretriz vinculativa, publicada sob a POPIA.

Estados Unidos:

Além das disposições do DPA, as Partes comprometem-se com o seguinte:

- a) Cada Parte reconhece e concorda que a coleta e divulgação de Dados Pessoais transmitidos aos Serviços de Processamento (i) não constituem, e não são a intenção de nenhuma das partes para que tal atividade constitua uma venda de Dados Pessoais, e (ii) se uma consideração valiosa, monetária ou não, está sendo fornecida pelo Usuário Autorizado ao Processador de Dados, tal consideração valiosa, monetária ou não, está sendo fornecida para uso dos Serviços de Processamento e não para a divulgação de Dados Pessoais. O Processador de Dados não deve reter, usar, divulgar ou vender Dados Pessoais para qualquer finalidade que não seja a finalidade específica de realizar os Serviços de Processamento, ou conforme permitido por lei ou pelo EULA. Para evitar dúvidas, o Processador de Dados não venderá Dados Pessoais ou autorizará, ou de qualquer outra forma, permitirá que qualquer Subprocessador faça o mesmo, a menos que de outra forma permitida pelo EULA ou lei aplicável.

Anexo 2 - Medidas de segurança implementadas pelo Processador de Dados**1. Controle de acesso físico às dependências e instalações**

O Processador de Dados implementará medidas técnicas e organizacionais para controlar o acesso às dependências e instalações, especialmente para verificar a autorização e garantir a prevenção de acessos não autorizados.

Especificamente:

- Sistema de controle de acesso
- Leitor de ID, cartão magnético, cartão com chip
- Emissão de chaves
- Travamento de porta
- Pessoal da segurança, guardas
- Instalações de vigilância
- Sistema de alarme, monitor de CFTV/vídeo

2. Controle de acesso aos sistemas

O Processador de Dados implementará medidas técnicas (segurança de senha/ID) e organizacionais para a identificação e autenticação do usuário para evitar o acesso não autorizado aos sistemas de TI.

Especificamente:

- Procedimentos de senha (incluindo caracteres especiais, comprimento mínimo, alteração de senha)
- Bloqueio automático (por exemplo, senha ou tempo limite)
- Criptografia de mídia de dados, incluindo removível e portátil.

3. Controle de acesso lógico aos dados

O Processador de Dados garantirá que as atividades em sistemas de TI não cobertas pelos direitos de acesso alocados serão evitadas, utilizando a definição orientada por requisitos do esquema de autorização e direitos de acesso, além de monitoramento e registro de acessos.

Especificamente:

- Direitos de acesso com base em cargos (perfis, funções, transações e objetos)
- Uso de uma solução comercial de Gerenciamento de Contas Privilegiadas para facilitar a autenticação segura de contas administrativas aos sistemas para manutenção ou outros fins administrativos
- Relatórios automatizados que são regularmente revisados e acompanhados para atividades anômalas ou suspeitas
- Acesso usando um modelo de privilégio mínimo para permitir apenas o acesso a sistemas e/ou dados somente a pessoas que precisem deles

4. Divulgação e controle de proteção de dados

O Processador de Dados controlará a divulgação de Dados Pessoais incorporando medidas para transportar, transmitir e comunicar ou armazenar dados em mídia de dados (manual ou eletrônica) e para verificação subsequente por transferência eletrônica, transporte de dados e controle de transmissão.

Especificamente:

- Criptografia/roteamento
- Assinatura eletrônica
- Registro e monitoramento contínuo de alertas e eventos de segurança
- Segurança de transporte para criptografar dados em trânsito
- Criptografia de dados armazenados
- Rotação regular de chaves de criptografia
- Restrição de acesso a chaves de criptografia para pessoas limitadas
- Complexidade de senha habilitada, com autenticação de dois fatores necessária para todas as sessões de acesso remoto

5. Controle de entrada

O Processador de Dados manterá a documentação completa de gerenciamento de dados e a manutenção deve ser registrada, incluindo medidas para verificar subsequentemente se os dados foram inseridos, alterados ou removidos (excluídos), e por quem:

Especificamente:

- Sistemas de relatórios e registro

6. Controle de trabalho

O Processador de Dados processará os Dados Pessoais de acordo com as instruções do Controlador de Dados e adotará as medidas (técnicas/organizacionais) para segregar as responsabilidades entre o Controlador de Dados e o Processador de Dados: Especificamente:

- Redação do contrato sem ambiguidades
- Comissionamento formal (formulário de solicitação)
- Critérios para selecionar o Processador de Dados
- Monitoramento da execução do contrato

7. Controle de disponibilidade

O Processador de Dados garantirá que os dados serão protegidos contra destruição ou perda acidental ou mal-intencionada, tomando medidas para garantir a segurança física e lógica dos dados.

Especificamente:

- Procedimentos de backup
- Espelhamento de discos rígidos, por exemplo, tecnologia RAID
- Fonte de alimentação ininterrupta (UPS)
- Armazenamento remoto ou baseado em disco que seja replicado para centros de dados alternativos
- Software antivírus e/ou antimalware que seja atualizado regularmente e sistemas de firewall com reconhecimento de aplicativo configurados com declarações de negação padrão, permitindo apenas o tráfego explicitamente permitido para fins comerciais
- Plano de Continuidade de Negócios e Recuperação de Desastres

8. Controle de Segregação

O Processador de Dados buscará garantir que os dados coletados para finalidades diferentes sejam processados separadamente e não combinados com outros dados do cliente, implementando medidas específicas para fornecer Processamento separado (armazenamento, alteração, exclusão, transmissão) de dados para finalidades diferentes:

Especificamente:

- Limitação de uso/Conceito de “cliente interno”
- Segregação de funções (produção/teste)