1.Objetivo:

Esta política tem como objetivos definir a metodologia para proteção de dados pessoais, bem e as tratativas em caso de vazamento.

2.Responsabilidades:

2.1. DPO

Definir a política de proteção de dados pessoais;

Analisar o **FE.A.06.1.5 DPIA - Data Protect Impact Assessment** de cada projeto ou processo de trabalho e realizar acompanhamento

Analisar o **FE.A.06.1.5 – Segurança da Informação no Gerenciamento de Projetos** de cada projeto ou processo de trabalho e realizar o acompanhamento

Verificar a atualização e conformidade do **FE.A.06.1.5 DPIA - Data Protect Impact Assessment** de acordo com a LGPD;

Gerenciar todas as atividades relacionadas a vazamento de dados;

Gerenciar a eliminação e destruição de dados;

Gerenciar o acesso aos dados pelos requerentes;

Controlar e monitorar a retenção de dados.

2.2. Diretoria

Apoiar o DPO nas ações para minimizar os riscos de vazamento e dados pessoais;

Apoiar o DPO nas tomadas de decisão em caso de vazamento de dados.

2.3. TI

Implementar quando sob sua responsabilidade as ações necessárias para minimizar os riscos de vazamento de dados;

Executar a retenção e eliminação de dados.

2.3. Compliance

Elaborar o **FE.A.06.1.5 DPIA - Data Protect Impact Assessment** e submeter à análise do DPO;

Elaborar o **FE.A.06.1.5 – Segurança da Informação no Gerenciamento de Projetos** e submeter à análise do DPO;

Implementar quando sob sua responsabilidade as ações necessárias para minimizar os riscos de vazamento de dados;

Executar a retenção e eliminação de dados

2.4. Gestores de Projetos

Realizar a análise de riscos dos projetos;

Implementar quando sob sua responsabilidade as ações necessárias para minimizar os riscos de vazamento de dados;

Realizar a análise de riscos na contratação de fornecedores;

Atender e suportar as solicitações realizados pelos requerentes de dados de acordo com regras estabelecidas na política ou previstas em lei;

2.5. Fornecedores e Terceiros

Conhecer e aplicar no tratamento dos dados pessoais o estabelecido nesta Política.

3.Proteção e Privacidade de Dados Pessoais

A Connect2B deve manter a integridade de todos os Dados Pessoais, garantindo que são precisos, completos e relevantes para os fins declarados para os quais foram processados.

3.1. Análise de riscos o projeto

Todo processo ou projeto da Connect2B deverá ser analisado, visando identificar os riscos relacionados à segurança da informação e vazamento de dados pessoais.

Esta análise deverá ser realizada pelo gestor do processo ou projeto, no **FE.A.06.1.5 – Segurança da Informação no Gerenciamento de Projetos**.

Se identificado a coleta, processamento, análise, compartilhamento, armazenamento, reutilização ou eliminação de dados pessoais ou sensíveis, deverá ser elaborado o DPIA, utilizando o **FE.A.06.1.5 DPIA - Data Protect Impact Assessment** de cada projeto visando identificar todos os riscos associados e os possíveis controles.

3.2. Elaboração do DPIA

A Connect2B define os procedimentos para validar os Dados Pessoais quando são recolhidos, criados e atualizados no **FE.A.06.1.5 DPIA - Data Protect Impact Assessment** de cada projeto ou processo de trabalho.

3.3. Cuidados com a subcontratação

No momento de contratação de um fornecedor para prestação de um serviço deverá ser realizada a análise dos riscos relacionados aos dados pessoais.

Se aplicável, deverá ser exigido os controles e garantias de proteção dos dados pessoais, mesmo após o término do contrato.

3.4. Monitoramento para contínua adequação

O DPO deverá analisar anualmente o **FE.A.06.1.5 DPIA - Data Protect Impact Assessment**, visando identificar a sua atualização e conformidade, sendo que a análise deverá ser documentada.

3.5. Cuidados com a subcontratação

O DPO deverá analisar qualquer fonte de vazamento e tomar as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito:

- **Medidas técnicas**:
  - Alteração de senhas;
  - Bloqueio de usuário;
  - Retirada do site do ar;
  - Formatação de computador ou celular;
  - Contratação de consultoria especializada (análise de vulnerabilidade), para identificar falhas.

- **Medidas administrativas**:
  - Informar a Diretoria da Connect2B;
  - Comunicar o cliente envolvido, quando aplicável;
  - Comunicar a ANDP;
  - Comunicar o titular sobre a ocorrência do incidente, que possam acarretar risco ou dano relevante aos titulares.

A comunicação será feita em prazo razoável, conforme definido pela ANPD, e deverá mencionar, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

3.6. Destruição/Eliminação de Dados

A eliminação/destruição dos dados será destruída por solicitação dos requerentes dos dados ou responsável pela coleta dos dados. O gestor do projeto junto com o DPO, irão assegurar que o a solicitação seja cumprida dentro do prazo estabelecido por lei ou determinado em contrato, desde que não exista conflito legal.

Somente será destruído o dado pessoal após a confirmação da propriedade ou responsabilidade pela coleta.

A solicitação deverá ser formalizada e a destruição será documentada com registros necessários.

Com relação ao prazo, o dado será destruído de acordo com prazo estabelecido:

- Por regras previstas em lei;
- De acordo com a política de privacidade prevista no momento do cadastro;
- Por condições de contrato entre as partes envolvidas;
- Pelo prazo previsto no **FE.A.06.1.5 DPIA - Data Protect Impact Assessment** de cada projeto ou processo de trabalho.

O dado armazenado em mídia física, o local de armazenamento será enviado para um fornecedor especializado e certificado em processo de destruição de mídias, caso seja necessário.

Todos os procedimentos poderão ser revistos caso exista conflito legal com lei vigente.

3.7. Acesso aos Dados pelo Requerentes

O acesso aos dados pelo requerente poderá ser feito no local de cadastro ou por solicitação formalizada e registrada.

Após as confirmações de segurança os dados do requerente serão disponibilizados por meio eletrônico de acordo com a solicitação.

O requerente dos dados poderá exercer seus direitos sobre os dados a qualquer momento, desde que por feita por solicitação formalizada para efeito de registro. Após confirmações de segurança, o direito solicitado será executado e registrado.

Somente será realizado acesso ou exercido de direito dos requerentes de dados, por meio formal e registrado para fins de documentação e evidência de execução.

A Connect2B controla o processamento de dados por projeto e utiliza ferramentas tecnológicas para garantir a varredura de dados dos requerentes no ambiente de armazenamento.

A documentação para registro de cumprimento terá:

- Data e hora do pedido;
- Ações tomadas para responder ao pedido;
- Demais registros que forem necessários.

A Connect2B fornecerá os dados em um formato compreensível e de forma prática para os requerentes de dados, sem codificação ou qualquer outra linguagem de sistema.

A solicitação de dados poderá ser negada caso exista algum conflito ou condição em que o pedido não possa ser executado. Haverá uma explicação consistente e razoável formalizada ao requerente dos dados.

Caso dados dos requerentes sejam de responsabilidade de terceiros, a Connect2B irá realizar a comunicação de pedidos ou procedimentos a todos os envolvidos formalizados, de acordo com padrões ou processos solicitados pelos responsáveis.

Todos os procedimentos poderão ser revistos caso exista conflito legal com lei vigente.

3.8. Retenção de Dados

Os dados armazenados pela Connect2B serão retidos somente pelo propósito que foi aprovado no **FE.A.06.1.5 DPIA - Data Protect Impact Assessment**. Eles são armazenados por projeto para permitir melhor controle, na forma que são recolhidos, criados e atualizados.

A integridade dos dados é suportada por ferramentas tecnológicas de armazenamento, com itens de segurança e conformidade que facilitam qualquer procedimento que for necessário para manutenção durante a retenção do dado.

4.Fornecedores

4.1. Obrigações legais da lei, tais como autorização para coleta, processamento e uso de dado e sua finalidade clara e objetiva.

O Fornecedor cumprirá, a todo momento, as leis de proteção de dados, jamais colocando, por seus atos ou por sua omissão, a Connect2B em situação de violação das leis de proteção de dados.

O Fornecedor somente poderá tratar Dados Pessoais conforme as instruções da Connect2B, a fim de cumprir suas obrigações com base no Contrato de Serviços, jamais para qualquer outro propósito.

O Fornecedor tratará os Dados Pessoais em nome da Connect2B e de acordo com as instruções escritas fornecidas. Caso o Fornecedor considere que não possui informações suficientes para o tratamento dos Dados Pessoais de acordo com o Contrato ou que uma instrução infringe as leis de proteção de dados, o Fornecedor prontamente notificará a Connect2B e aguardará novas instruções.

O Fornecedor se certificará que seus empregados, representantes, e prepostos agirão de acordo com o Contrato, as leis de proteção de dados e as instruções transmitidas pela Connect2B. O Fornecedor se certificará que as pessoas autorizadas a tratar os Dados Pessoais assumam um compromisso de confidencialidade ou estejam sujeitas a adequadas obrigações legais de confidencialidade.

Se o titular dos dados, autoridade de proteção de dados, ou terceiro solicitarem informações do Fornecedor relativas ao tratamento de Dados Pessoais, o Fornecedor submeterá esse pedido à apreciação da Connect2B. O Fornecedor não poderá, sem instruções prévias da Connect2B, transferir ou, de qualquer outra forma, compartilhar e/ou garantir acesso aos Dados Pessoais ou a quaisquer outras informações relativas ao tratamento de Dados Pessoais a qualquer terceiro.

O Fornecedor prontamente prestará assistência à Connect2B no sentido de assegurar o cumprimento da obrigação de responder às solicitações dos titulares de dados, incluindo pedidos de acesso, retificação, bloqueio, restrição, apagamento, portabilidade de dados, ou o exercício de quaisquer outros direitos dos titulares de dados com base nas Leis Aplicáveis à Proteção de Dados.

O Fornecedor também assistirá à Connect2B por meio da implementação das devidas medidas

técnicas e organizacionais sugeridas pelo Fornecedor, para que a Connect2B possa cumprir suas obrigações de responder a tais pedidos.

4.2. Segurança do dado armazenado

O Fornecedor implementará as medidas técnicas e organizacionais apropriadas para proteger os Dados Pessoais, levando em conta as técnicas mais avançadas, o custo de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos apresentados pelo processamento, em particular, devidos à destruição, perda, alteração ou divulgação não-autorizada dos Dados Pessoais, de forma acidental ou ilegal, ou ao acesso aos Dados Pessoais transmitidos, armazenados, ou de outra forma tratados.

As medidas de segurança do Fornecedor atenderão ou excederão as:

- exigências das leis de proteção de dados e
- medidas de segurança correspondentes com as boas práticas do ramo de negócios do Fornecedor

4.3. Política em caso de vazamento de dados

Na hipótese de uma violação de Dados Pessoais, o Fornecedor informará a Connect2B, por escrito, acercada violação dos Dados Pessoais, em prazo não superior a imediatamente a contar do momento em que tomou ciência da violação.

As informações a serem disponibilizadas pelo Fornecedor incluirão:

- descrição da natureza da violação dos Dados Pessoais, incluindo as categorias e o número aproximado de titulares de dados implicados, bem como as categorias e o número aproximado de registros de dados implicados;
- descrição das prováveis consequências ou das consequências já concretizadas da violação dos Dados Pessoais; e
- descrição das medidas adotadas ou propostas para reparar a violação dos Dados Pessoais e mitigar os possíveis efeitos adversos.

4.4. Transferência de Dados

O Fornecedor não poderá transferir Dados Pessoais para fora do Brasil, da UE ou do EEE nem terceirizar, para uma subcontratada, o tratamento de Dados Pessoais sem a devida aprovação, por escrito, da Connect2B.

Se for aprovada a contratação de outras subcontratadas, o Fornecedor assegurará que tais subcontratadas assumam contratualmente o cumprimento de obrigações correspondentes às obrigações contidas nesta Política.

Nos casos em que uma subcontratada deixar de cumprir sua obrigação de proteger os dados, o Fornecedor será responsável perante a Connect2B pelo cumprimento das obrigações da subcontratada.

Se a Connect2B aprovar a utilização de outras subcontratadas, o Fornecedor, prontamente, informará a Connect2B, por escrito, de quaisquer mudanças pretendidas relativas à adição ou substituição dessas subcontratadas, dando a Connect2B, dessa forma, a oportunidade de impugnar essas mudanças.

Caso a Connect2B venha a impugnar essas mudanças, o Fornecedor não procederá com a utilização das subcontratadas. Os conhecimentos obtidos da análise e resolução de incidentes de segurança da informação e privacidade são usados para reduzir a probabilidade ou impacto de incidentes futuros.

4.5. Responsabilidades e Indenização

O Fornecedor e seus subcontratados poderão ser responsabilizadas por quaisquer multas impostas por autoridades de proteção de dados como pena por violarem a lei de proteção de dados.

Histórico de Alterações

Rev	Data	Histórico	Aprovado por
00	01/08/2019	Emissão	Germano Demary - DPO
01	31/07/2020	Revisão e Análise Geral	Germano Demary - DPO
02	01/03/2021	Revisão e Análise Geral Atualização Responsabilidades Atualização Nomenclaturas Inclusão do Item Fornecedores	Germano Demary - DPO