POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

AGRESTIPREV 2023

APRESENTAÇÃO

Nos últimos anos, a crescente digitalização das informações e o aumento do uso de tecnologias têm levado à necessidade de proteger de forma mais eficaz os dados pessoais dos indivíduos. Nesse contexto, a Lei nº. 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) surge como um marco regulatório essencial para garantir a privacidade e a segurança das informações no ambiente digital. A aplicação da LGPD torna-se ainda mais relevante em um Regime Próprio de Previdência, onde dados sensíveis dos segurados e beneficiários são coletados, armazenados e processados.

A LGPD estabelece diretrizes e regras claras para a coleta, uso, armazenamento e compartilhamento de dados pessoais, garantindo que as informações sejam tratadas de forma adequada e respeitando a privacidade dos indivíduos. No contexto dos RPPS, a adoção de medidas de proteção de dados é fundamental, uma vez que esses regimes possuem acesso a informações sensíveis, como dados financeiros, de saúde e informações pessoais dos segurados.

Um dos principais objetivos da LGPD é assegurar que os titulares dos dados tenham controle sobre suas informações e que seu tratamento seja feito de maneira segura e transparente. No âmbito dos RPPS, isso implica em adotar práticas e políticas que garantam a proteção dos dados pessoais, incluindo a implementação de medidas de segurança adequadas, como criptografia, controle de acesso e monitoramento de dados.

Além disso, a LGPD exige que os RPPS informem de forma clara e transparente aos segurados sobre a finalidade da coleta de seus dados, bem como sobre como esses dados serão utilizados e compartilhados. Isso proporciona maior confiança e transparência aos segurados, fortalecendo o relacionamento entre o regime previdenciário e seus beneficiários.

Outro aspecto relevante é que a LGPD estabelece sanções e penalidades para o descumprimento das normas de proteção de dados. Dessa forma, os

RPPS têm o dever de estar em conformidade com a lei, evitando possíveis sanções e prejuízos financeiros e reputacionais. A conformidade com a LGPD contribui para o fortalecimento da imagem do regime previdenciário, demonstrando o compromisso com a segurança e privacidade dos dados dos segurados.

Em suma, a aplicação da Lei Geral de Proteção de Dados em um Regime Próprio de Previdência é de suma importância para garantir a segurança, privacidade e transparência no tratamento das informações pessoais dos segurados. A adoção de práticas e políticas que estejam em conformidade com a LGPD fortalece o relacionamento entre o regime previdenciário e seus beneficiários, além de evitar possíveis sanções legais.

Instituto de Previdência dos Servidores Municipais de Agrestina - AGRESTIPREV

DIRETORIA EXECUTIVA

ROBERTO MARCELO BORBA ALVES
Diretor Presidente

VALDEMIR MOREIRA DA SILVA
Diretor Financeiro e de Investimentos

CHRISTIANNE ALVES BATISTA TAVARES
Gerente Administrativo de Previdência e de Benefícios

ANA CLARA ALVES DOS SANTOS VASCONCELOS
Presidente do Conselho Municipal de Previdência

INTRODUÇÃO

A Lei nº. 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que entrou em vigor em agosto de 2018 e tem como objetivo principal estabelecer regras claras e abrangentes para o tratamento de dados pessoais no país. A LGPD foi criada em resposta à crescente preocupação com a privacidade e a segurança das informações pessoais, impulsionada pela rápida evolução tecnológica e pela necessidade de proteger os direitos dos indivíduos no ambiente digital.

A visão geral da LGPD é proporcionar maior controle e transparência aos titulares dos dados sobre como suas informações são coletadas, armazenadas, usadas e compartilhadas por empresas e organizações. Ela estabelece diretrizes claras para o tratamento adequado dos dados pessoais, independentemente do meio em que são processados, seja digital ou físico.

Os princípios básicos defendidos pela LGPD são fundamentais para garantir a proteção dos direitos dos indivíduos. O princípio da finalidade estabelece que os dados pessoais devem ser coletados para propósitos legítimos, específicos e informados aos titulares, evitando-se o uso excessivo ou não autorizado dessas informações.

Outro princípio importante é o da adequação, que determina que o tratamento dos dados deve ser limitado ao necessário para o cumprimento da finalidade informada aos titulares. Isso implica em minimizar a coleta de dados e garantir que apenas as informações relevantes sejam utilizadas.

A LGPD também enfatiza o princípio da necessidade, que assegura que apenas os dados estritamente necessários para a finalidade informada devem ser coletados, evitando-se a obtenção de informações excessivas ou desnecessárias.

Além disso, a legislação ressalta o princípio do livre acesso, que garante aos titulares o direito de acessar suas informações pessoais, bem como solicitar a correção, exclusão ou portabilidade desses dados.

Outro princípio fundamental é o da segurança, que exige a adoção de medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, perda, destruição ou divulgação indevida.

Por fim, a LGPD estabelece o princípio da prestação de contas, que exige que as organizações demonstrem que estão em conformidade com a lei, mantendo registros de suas atividades de tratamento de dados.

TERMINOLOGIAS

A Lei Geral de Proteção de Dados (LGPD) utiliza uma série de termos importantes para definir conceitos e estabelecer direitos e responsabilidades relacionados à proteção de dados pessoais. A seguir, estão alguns dos termos mais relevantes e suas explicações:

1. **Dado pessoal:** Refere-se a qualquer informação relacionada a uma pessoa física identificada ou identificável. Pode incluir dados como nome, endereço, CPF, RG, entre outros.
2. **Dado pessoal sensível:** São dados que revelam informações mais íntimas e sensíveis sobre uma pessoa, como origem racial ou étnica, convicções religiosas, opiniões políticas, saúde, orientação sexual, entre outros. O tratamento desses dados é sujeito a restrições adicionais.
3. **Tratamento de dados:** Compreende todas as operações realizadas com os dados pessoais, como coleta, armazenamento, uso, compartilhamento, transferência, entre outros.
4. **Controlador:** É a pessoa física ou jurídica, de direito público ou privado, que toma as decisões sobre o tratamento de dados pessoais, definindo as finalidades, os meios e os limites para esse tratamento.
5. **Operador:** É a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador, seguindo suas instruções.
6. **Titular dos dados:** É a pessoa física a quem os dados pessoais se referem, ou seja, o indivíduo que é identificado ou identificável a partir desses dados.

7. **Consentimento:** Refere-se à manifestação livre, informada e inequívoca do titular dos dados concordando com o tratamento de seus dados pessoais para uma finalidade específica.
8. **Anonimização:** É o processo pelo qual os dados pessoais são transformados de forma a não permitir a identificação direta ou indireta do titular, tornando-os irreversíveis.
9. **Encarregado de proteção de dados (DPO):** É a pessoa indicada pelo controlador ou operador para atuar como ponto de contato entre o RPPS, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), garantindo o cumprimento da LGPD.
10. **Autoridade Nacional de Proteção de Dados (ANPD):** É a entidade governamental responsável pela regulamentação, orientação, fiscalização e aplicação da LGPD no Brasil.

DOS DIREITOS E DEVERES

Consciência da importância da proteção de dados: Os titulares dos dados devem estar cientes da relevância da proteção dos dados pessoais e compreender que suas informações estão sendo tratadas em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Conhecer a Política, assinando o Termo de Ciência: Todos que fazem parte do AGRESTIPREV devem ler atentamente este documento e assinar o Termo de Ciência contante no Anexo I.

Fornecer dados precisos e atualizados: É dever dos titulares dos dados fornecerem informações precisas, completas e atualizadas no momento do seu cadastro ou solicitação de benefícios no Instituto de Previdência dos Servidores Municipais de Agrestina – AGRESTIPREV.

Utilização responsável dos dados: Os titulares dos dados, sejam eles servidores efetivos, cargos comissionados, contratados ou prestadores de serviços devem utilizar as informações fornecidas somente para os fins legítimos e de acordo com as finalidades comunicadas no momento da coleta.

Manter sigilo e confidencialidade: Os servidores efetivos, cargos comissionados, contratados ou prestadores de serviços têm a responsabilidade de manter a confidencialidade de suas informações pessoais, não compartilhando suas senhas de acesso com terceiros e evitando a exposição desnecessária de seus dados.

Comunicar alterações e retificar informações: É importante que os titulares dos dados informem aos responsáveis pelo Instituto de Previdência dos Servidores Municipais de Agrestina – AGRESTIPREV sobre eventuais alterações em seus dados pessoais, a fim de garantir que as informações estejam sempre atualizadas. Além disso, caso identifiquem dados imprecisos, incompletos ou desatualizados, devem solicitar a retificação dessas informações.

Exercer os direitos garantidos pela Lei nº. 13.709/2018 – LGPD: Os titulares dos dados têm o direito de exercer seus direitos estabelecidos pela LGPD, como o acesso aos dados, a retificação, a exclusão e a portabilidade de suas informações. É importante que eles estejam cientes desses direitos e saibam como exercê-los junto ao Instituto de Previdência dos Servidores Municipais de Agrestina – AGRESTIPREV.

Reportar incidentes de segurança: Caso os titulares dos dados suspeitem de qualquer incidente de segurança ou acesso não autorizado às suas informações, é fundamental que eles reportem imediatamente ao RPPS através da Ouvidoria no e-mail: ouvidoriaagrestiprev@hotmail.com, a fim de que medidas sejam tomadas para mitigar os possíveis danos.

Colaborar com a segurança dos dados: Os titulares dos dados devem colaborar com as medidas de segurança adotadas pelo AGRESTIPREV, seguindo as orientações fornecidas e adotando boas práticas de segurança, como o uso de senhas fortes e a proteção de dispositivos utilizados para acessar os sistemas do RPPS.

Conhecer a política de privacidade: Os titulares dos dados devem ter conhecimento da política de privacidade do AGRESTIPREV, compreendendo como suas informações são coletadas, armazenadas, utilizadas e

compartilhadas, bem como quais são as medidas de segurança adotadas para protegê-las.

DAS RESPONSABILIDADES

Como encarregado de acompanhar a execução da Lei Geral de Proteção de Dados (LGPD) no Instituto de Previdência dos Servidores Municipais de Agrestina – AGRESTIPREV, no Município de Agrestina/PE, o Diretor Presidente possui uma série de responsabilidades. Essas responsabilidades incluem:

1. **Conhecimento da LGPD:** O Diretor Presidente deve ter um conhecimento aprofundado da Lei nº. 13.709/2018 – LGPD, compreendendo os seus princípios, diretrizes e requisitos para garantir a conformidade do RPPS com a legislação.
2. **Avaliação da conformidade:** É responsabilidade do Diretor Presidente avaliar a conformidade do RPPS com a LGPD, verificando se as práticas e políticas adotadas estão de acordo com as exigências da lei.
3. **Implementação de políticas e procedimentos:** O Diretor Presidente deve desenvolver e implementar políticas e procedimentos internos que orientem o tratamento de dados pessoais no RPPS, garantindo a proteção da privacidade e segurança das informações.
4. **Nomeação de um encarregado de proteção de dados**: O Diretor Presidente é responsável por nomear um encarregado de proteção de dados (DPO) dentro do Instituto de Previdência dos Servidores Municipais de Agrestina - AGRESTIPREV, que será responsável por garantir o cumprimento da LGPD e atuar como ponto de contato entre, o RPPS, os titulares dos dados. Na ocasião da elaboração desta PSI, foi designado o Sr. Valdemir Moreira da Silva – Diretor Financeiro e de Investimentos.
5. **Treinamento e conscientização:** O Diretor Presidente deve promover treinamentos e programas de conscientização para os servidores do RPPS, a fim de garantir que todos compreendam a importância da

proteção de dados e estejam cientes das responsabilidades e boas práticas necessárias para cumprir a LGPD.

6. **Análise de impacto de proteção de dados (AIPD):** É responsabilidade do Diretor Presidente conduzir análises de impacto de proteção de dados, quando necessário, avaliando os riscos e impactos do tratamento de dados no RPPS e implementando medidas para mitigar esses riscos.
7. **Resposta a incidentes:** O Diretor Presidente deve estabelecer procedimentos de resposta a incidentes de segurança que possam comprometer a proteção dos dados no RPPS, garantindo ações rápidas e eficientes para minimizar danos e informar as partes envolvidas.
8. **Atendimento a solicitações dos titulares:** O Diretor Presidente é responsável por garantir que as solicitações dos titulares de dados, como acesso, retificação ou exclusão, sejam adequadamente atendidas dentro dos prazos. As solicitações devem ser realizadas pela Ouvidoria, e terão um prazo de 30 dias para serem atendidos.
9. **Auditoria e monitoramento:** O Diretor Presidente deve realizar auditorias internas e monitorar periodicamente o cumprimento das políticas e procedimentos relacionados à proteção de dados, assegurando a conformidade contínua com a LGPD.

TRATAMENTO DE DADOS SENSÍVEIS

Identificar dados sensíveis: O RPPS deve identificar quais dados são considerados sensíveis de acordo com a LGPD. Essa identificação é fundamental para aplicar medidas específicas de proteção.

Adotar medidas de segurança: O Instituto de Previdência dos Servidores Municipais de Agrestina – AGRESTIPREV deve implementar medidas de segurança adequadas para proteger os dados sensíveis, como criptografia, controle de acesso, monitoramento de atividades, entre outras.
Essas medidas devem ser proporcionais ao risco envolvido no tratamento dos dados sensíveis.

Limitar o acesso: É importante restringir o acesso aos dados sensíveis apenas a colaboradores autorizados que necessitam dessas informações para o desempenho de suas funções. O RPPS deve estabelecer políticas de acesso e controle para evitar o acesso não autorizado.

Realizar auditorias de segurança: O AGRESTIPREV deve realizar auditorias regulares para avaliar a eficácia das medidas de segurança implementadas. Essas auditorias ajudam a identificar possíveis vulnerabilidades e garantir que os dados sensíveis estejam adequadamente protegidos.

Treinamento e conscientização: Todos os colaboradores do Instituto de Previdência dos Servidores Municipais de Agrestina – AGRESTIPREV devem receber treinamento e conscientização sobre a importância da proteção de dados sensíveis, bem como sobre as políticas e procedimentos estabelecidos para seu tratamento.

Monitoramento e resposta a incidentes: O AGRESTIPREV deve implementar um sistema de monitoramento contínuo para identificar e responder a incidentes de segurança que possam afetar os dados sensíveis. Manter o software do sistema e antivírus atualizados e senhas individuais de acesso aos sistemas.

ROBERTO MARCELO BORBA ALVES
Diretor Presidente

ANA CLARA ALVES DOS SANTOS VASCONCELOS
Presidente do Conselho Municipal de Previdência