Área Gestora:
Gerência de Tecnologia da Informação

Data da Aprovação:
26/10/2021

SUMÁRIO

1. OBJETIVO **2**
2. APLICAÇÃO **2**
3. REFERÊNCIAS **2**
4. DEFINIÇÕES **2**
5. PRINCÍPIOS GERAIS **3**
5.1. Tratamento de Dados Pessoais **4**
5.2. Coleta de Dados Pessoais **5**
5.2.1. Coleta de Dados Pessoais de Crianças e Adolescentes 5
5.3. Do Compartilhamento de Dados Pessoais **5**
5.3.1. Do Nível de Compartilhamento de Dados Pessoais 5
5.3.2. Dos Cuidados no Compartilhamento de Dados Pessoais 6
5.4. Transferência Internacional **7**
5.5. Eliminação de Dados Pessoais **7**
5.6. *Data Protection Officer* - DPO (Encarregado) **7**
5.7. Direitos dos Titulares e Canal de Gerenciamento de Solicitações **8**
5.8. Relatório de Impacto à Proteção de Dados Pessoais **8**
5.9. Privacy by Design **8**
5.10. Comitê de Governança de Dados Pessoais **8**
5.11. Boas Práticas para Governança e Proteção de Dados Pessoais **9**
6. RESPONSABILIDADES **9**
6.1. Da Diretoria Executiva **9**
6.2. Da Gerência de Tecnologia da Informação **10**
6.3. Da Gerência de Governança, Riscos e Compliance **10**
6.4. Da Gerência de Gestão de Pessoas **10**
6.5. Da Gerência Jurídica **10**
6.6. Do(a) *Data Protection Officer* **10**
6.7. Das demais gerências e colaboradores **11**
7. ANEXOS **11**

1. OBJETIVO

Consolidar os princípios e práticas de proteção e governança de dados pessoais adotados pela Fundação de Seguridade Social Braslight (“entidade”) em observância aos preceitos da Lei nº 13.709, de 14 de agosto de 2019 - Lei Geral de Proteção de Dados Pessoais (“LGPD”), em adição às disposições contratuais e práticas relativas ao sigilo e à confidencialidade.

A LGPD regula o tratamento de dados pessoais, nos meios digitais ou físicos, realizado por pessoas naturais ou jurídicas, de direito público ou privado, visando proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da pessoa natural.

Em aderência à LGPD, o presente Normativo dispõe sobre os preceitos básicos da lei e os procedimentos que deverão ser observados em todas as atividades que envolvam a coleta, o acesso ou o tratamento de dados pessoais de participantes, assistidos, beneficiários, colaboradores, diretores, conselheiros, prepostos da entidade, bem como de quaisquer outras pessoas físicas cujos dados se tornem acessíveis em razão das atividades realizadas.

Este Normativo busca garantir a proteção dos dados pessoais acessíveis no âmbito das operações da entidade, assegurando que sejam sempre tratados em observância aos princípios da boa-fé, finalidade, adequação e necessidade, bem como livre acesso, segurança, prevenção e não discriminação, de modo a preservar a transparência ao titular dos dados sobre o tratamento de seus dados pessoais, conforme as melhores práticas de governança e mitigação de riscos.

2. APLICAÇÃO

O presente Normativo aplica-se aos colaboradores, prepostos, diretores, conselheiros, fornecedores e parceiros da Braslight que atuem em seu nome nas atividades e funções que envolvam dados pessoais sob controle da entidade.

3. REFERÊNCIAS

- Política de Proteção de Dados Pessoais
- Manual de Controles de Sistema de Gestão da Segurança da Informação
- Política de Segurança da Informação

4. DEFINIÇÕES

- **Agentes de tratamento de dados:** controlador, pessoa natural ou jurídica, de direito público ou privado, a quem compete a tomada de decisões referentes ao tratamento de dados pessoais, e o operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome ou a pedido do controlador;

- **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD;
- **Dado pessoal:** informação que, isolada ou associada a outras, identifique ou que possa identificar uma pessoa natural;
- **Dado pessoal sensível:** informação sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Dado pseudonimizado:** informação sobre um titular de dados que somente o identifica quando associada a informação adicional relativa ao titular, mantida separadamente pelo controlador em ambiente controlado e seguro;
- **Encarregado (ou *Data Protection Officer* - DPO):** pessoa indicada pelo controlador ou operador encarregado para atuar como canal de comunicação com titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD);
- **Titular dos dados pessoais:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, inclusive participantes, assistidos, beneficiários, colaboradores, conselheiros, diretores, fornecedores – quando pessoas físicas - e demais prepostos da entidade;
- **Tratamento de dados pessoais:** operação realizada com dados pessoais, que abarca a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados pessoais.

5. PRINCÍPIOS GERAIS

Todo e qualquer tratamento de dados pessoais no âmbito da entidade ou mediante solicitação desta, deverá ser realizado de acordo com as regras e procedimentos estipulados em normas relativas à proteção de dados pessoais, e pautadas na boa-fé, lealdade, respeito e transparência ao tratamento dos dados pessoais, e nos seguintes princípios:

- **Finalidade:** os dados pessoais coletados e processados são utilizados para realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, não sendo utilizados de forma incompatível com tais objetivos;

- **Adequação:** os dados pessoais são tratados em compatibilidade com as finalidades informadas ao seu titular ou pertinentes ao contrato por ele firmado com a entidade, no contexto do tratamento realizado;

- **Necessidade:** o tratamento deve se limitar ao mínimo possível de dados pessoais indispensáveis à realização das finalidades objetivadas, observada a sua pertinência e proporcionalidade;

- **Livre acesso:** é assegurada aos titulares a realização de consulta facilitada e gratuita sobre os seus dados pessoais tratados, bem como sobre a forma e a duração do seu tratamento;

- **Qualidade dos dados:** os dados pessoais tratados devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento;

- **Transparência:** é assegurado ao titular de dados pessoais o acesso a informações precisas e facilitadas sobre o tratamento de seus dados pessoais e os respectivos agentes de tratamento;

- **Segurança:** são aplicáveis para tratamento de dados todas as medidas 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 difusão;

- **Prevenção:** são aplicáveis para tratamento de dados pessoais todas as medidas técnicas, operacionais e contratuais adequadas para prevenir eventual ocorrência de danos ou riscos em virtude das atividades de tratamento de dados pessoais;

- **Não discriminação:** é vedada a realização de tratamento de dados pessoais para qualquer forma de discriminação ilícita ou abusiva;

- **Responsabilização e prestação de contas:** para garantia de proteção de dados pessoais, poderá haver demonstração das medidas e providência preventivas adotadas pela entidade.

5.1. Tratamento de Dados Pessoais

Todo e qualquer tratamento de dados realizado no âmbito da entidade, ou a pedido desta, deve ter por preceito mínimo a observância aos princípios indicados neste Normativo, mesmo nos casos em que o tratamento seja baseado em consentimento fornecido pelo titular, para execução de contrato ou procedimentos preliminares ao contrato, cumprimento de obrigação legal ou regulatória, para exercício regular do direito em processo judicial, administrativo ou arbitral, ou em razão do legítimo interesse da entidade.

Na ocorrência de tratamento com base em legítimo interesse, são requisitos indispensáveis:

- A proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais;

- Utilização dos dados pessoais estritamente necessários para o atendimento à finalidade pretendida;

- Adoção das medidas para garantir, ao titular, a transparência do referido tratamento de dados.

5.2. Coleta de Dados Pessoais

A coleta de dados pessoais deve ser destinada a atender propósitos específicos e legítimos, observada limitação aos dados pessoais mínimos necessários para atendimento às respectivas finalidades, de modo a assegurar que:

- O titular dos dados pessoais seja informado em contrato, telefone, e-mail, mensagem, pessoalmente ou outro, de maneira clara e específica sobre como seus dados serão tratados e para quais finalidades;
- O tratamento é adequado ao contexto em que os dados pessoais foram coletados; e
- A indispensabilidade dos dados pessoais coletados para atingir aquela finalidade pretendida.

5.2.1. Coleta de Dados Pessoais de Crianças e Adolescentes

Na coleta de dados de crianças e adolescentes, inclusive beneficiários dos planos de benefícios e dependentes de colaboradores e diretores da entidade, deverão ser adotados procedimentos para certificar que a coleta de dados e o consentimento para o tratamento de dados é realizado diretamente pelos pais ou responsáveis legais.

Observada a legislação que rege às operações de previdência e as informações necessárias para operacionalização do escopo dos contratos firmados com a entidade, dados pessoais de participantes e/ou beneficiários maiores de 17 (dezessete) anos não poderão ser disponibilizados a terceiros.

5.3. Do Compartilhamento de Dados Pessoais

5.3.1. Do Nível de Compartilhamento de Dados Pessoais

Em observância à classificação de ativos de informação constante no Manual de Controles de Sistema de Gestão da Segurança da Informação (confidencial, restrita e pública), o compartilhamento de dados pessoais na entidade é classificado em três níveis, de acordo com a categoria e a confidencialidade dos dados, bem como o enquadramento do tratamento realizado:

- Compartilhamento amplo, quando se tratar de dados públicos ou tornados manifestamente públicos pelo titular (informação pública), que não estão sujeitos a restrição de acesso e compartilhamento, resguardados os diretos do titular dos dados e os princípios estabelecidos neste Normativo e na LGPD;

- Compartilhamento restrito, quando se tratar de dados pessoais coletados ou disponibilizados para o cumprimento de contrato e seus procedimentos preliminares ou para o cumprimento de obrigação legal ou regulatória (informação confidencial);

- Compartilhamento específico, quando se tratar de compartilhamento de dados confidenciais e/ou sigilosos ou dados sensíveis e dados de crianças e adolescentes (informação confidencial).

O compartilhamento de dados ocorrerá com base no disposto nos itens 5.3.1 e 5.3.2 deste Normativo, devendo, o receptor dos dados, garantir o adequado tratamento e segurança dos dados pessoais recepcionados.

O compartilhamento de dados pessoais com base do legítimo interesse do controlador enquadra-se em compartilhamento específico de dados, devendo, nestes casos, o tratamento e compartilhamento serem precedidos de comunicação prévia ao DPO, com observância aos preceitos contidos no item 5.1 deste Normativo.

5.3.2. Dos Cuidados no Compartilhamento de Dados Pessoais

As disposições gerais deste item são aplicáveis em qualquer hipótese de compartilhamento de dados pessoais pela entidade ou pelos fornecedores e parceiros, independentemente do enquadramento de categoria.

O compartilhamento de dados pessoais pela entidade deve ocorrer apenas quando houver consentimento do seu titular ou quando seja necessário à realização do tratamento previamente autorizado pelo titular, inclusive por decorrência de contratos firmados com a entidade.

Os contratos e convênios com terceiros, para os quais haja o compartilhamento de dados pessoais, devem conter cláusulas específicas dispondo sobre a observância à proteção e governança de dados pessoais e medidas de minimização de riscos.

5.3.3. Do compartilhamento de dados com a administração pública

Nos casos em houver o recebimento de informações constantes em bases de dados controlados pela Administração Pública, a entidade deverá se assegurar, além do atendimento das finalidades e princípios compatíveis com as atividades realizadas pela entidade, que:

(i) Se trate de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação (Lei nº 12.527/18);

(ii) Nos casos em que os dados forem acessíveis publicamente;

(iii) Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;

(iv) Na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

5.4. Transferência Internacional

Nos casos em que se fizer necessária a realização de transferência internacional de dados pessoais, é cabível conferir previamente a existência, no país de destino, de norma ou dever de proteção de dados pessoais, em observância ao fiel cumprimento das disposições e requisitos estabelecidos neste Normativo e na LGPD.

5.5. Eliminação de Dados Pessoais

O tratamento e armazenamento de dados pessoais somente estão autorizados pelo período necessário à realização das finalidades que motivaram a coleta e tratamento de tais dados, bem como para cumprimento de obrigações contratuais e legais, observada a sua indisponibilidade, quando do término do tratamento, em sistemas, redes ou pastas físicas da entidade.

Os dados pessoais e ou dados pessoais sensíveis tratados pela entidade devem ser mantidos enquanto existir relação jurídica com o respectivo titular, exceto nos casos em que, por observância a legislação ou regulamentação, seja necessária a conservação por prazo superior, findo o qual os dados pessoais serão eliminados.

A eliminação de documentos contendo dados pessoais deverá seguir o procedimento especificado na tabela de temporalidade da entidade.

Havendo determinação por parte de autoridade pública ou judicial para a manutenção de informações relacionadas a pessoas físicas, a entidade deverá atender ao mandamento, procedendo com a exclusão após passado o período determinado.

5.6. *Data Protection Officer* - DPO (Encarregado)

A entidade indicará o DPO, em deliberação da Diretoria Executiva, como responsável pelo canal de comunicação entre a entidade, os titulares de dados pessoais (participantes, assistidos, beneficiários, colaboradores, fornecedores, dirigentes e prepostos), partes interessadas e a ANPD, deve prestar os esclarecimentos necessários sobre este Normativo e sua aplicação, casos excepcionais e boas práticas a serem adotadas permanentemente por colaboradores, diretores conselheiros, fornecedores e parceiros da entidade.

Eventuais incidentes de vazamentos ou riscos de exposição de dados pessoais tratados pela entidade deverão ser reportados ao DPO com a máxima brevidade possível para que adote plano de contenção e remediação dos seus efeitos, inclusive quanto a:

- Providências voltadas à prevenção de danos e mitigação de riscos envolvendo dados pessoais, considerando o incidente de segurança havido e seus reflexos, inclusive quanto a:
- Os procedimentos internos adotados;

- A exposição de risco e vulnerabilidades relevantes;
- A necessidade de treinamento, capacitação e aprimoramento na cultura organizacional;
- Alteração de fornecedores, instituidores e patrocinadores, ou procedimentos com eles adotados;
- Quantificação dos custos envolvidos (legais, internos, de remediação e intangíveis);
- Mensuração contingencial dos danos potenciais;
- Demais fatores relevantes.

5.7. Direitos dos Titulares e Canal de Gerenciamento de Solicitações

É assegurado o acesso facilitado e claro às informações sobre o tratamento de dados pessoais realizados pela entidade, sempre que solicitado pelo titular dos dados.

As solicitações relativas aos direitos de privacidade e proteção de dados dos titulares deverão ser efetuadas e encaminhadas ao canal de gerenciamento de solicitações, conduzido pelo DPO.

Devem ser adotados procedimentos de identificação e autenticação das solicitações realizadas, atendendo somente após confirmada a identidade do titular, ainda que se necessário a solicitação de documentos adicionais para tal atendimento.

5.8. Relatório de Impacto à Proteção de Dados Pessoais

Nos casos em que o tratamento de dados oferecer riscos às liberdades civis e aos direitos fundamentais do titular, é cabível a elaboração de relatório de impacto à proteção de dados pessoais, contendo a descrição dos processos de tratamento de dados pessoais e as medidas, salvaguardas e mecanismos de mitigação de risco adotados.

5.9. Privacy by Design

A todo projeto ou operação desenvolvido pela ou sob demanda da entidade devem ser incorporados os conceitos e práticas de privacy by design (privacidade desde a concepção), para garantia da governança e proteção dos dados pessoais do usuário.

5.10. Comitê de Governança de Dados Pessoais

O Comitê formado pela entidade, é composto pelo Encarregado (DPO), pelo responsável pela área de controle de processos da entidade, pelo responsável pela Tecnologia da Informação da entidade, e por um indicado pelo Conselho Deliberativo.

O Comitê terá o papel de deliberar sobre as atividades de tratamento da entidade, auxiliar o Encarregado no desempenho de suas funções, e promover a conscientização interna sobre os procedimentos envolvendo dados pessoais e segurança da informação.

5.11. Boas Práticas para Governança e Proteção de Dados Pessoais

Além da observância aos preceitos e regras contidas neste Normativo e na Política de Segurança da Informação, inclusive aos princípios de “Mesa e Tela Limpas”, deverão ser adotadas medidas de boas práticas que assegurem a proteção e a governança de dados pessoais, inclusive para que:

- As solicitações de áreas internas, fornecedores e parceiros sejam atendidos, sempre que possível, sem a identificação dos titulares de dados pessoais ou mediante pseudonimização;
- Dados pessoais não sejam expostos em reuniões de comissões, comitês e grupos de trabalho;
- Titulares de dados pessoais não sejam identificados em reuniões dos Conselhos Deliberativo e Fiscal quando não for essencial à análise dos assuntos sob debate ou deliberação de tais órgãos de governança, mantida a pseudonimização;
- Arquivos contendo dados pessoais não sejam impressos, exceto quando imprescindível para assinatura ou outra providência que não possa ser realizada sem que haja impressão dos dados pessoais – hipótese em que os papéis devem ser destruídos após o seu tratamento ou atingimento de finalidade, na forma prevista neste Normativo;
- Papéis, arquivos, dossiês e pastas físicas contendo dados pessoais sejam guardados com segurança e não sejam reutilizados, ainda que para rascunho;
- Haja o registro das operações de tratamento de dados pessoais e dados pessoais sensíveis realizadas pelos operadores de dados pessoais (fornecedores) em seu nome;
- Sejam utilizados mecanismos para assegurar que o contato telefônico está sendo realizado diretamente com o titular de dados ou seu representante legal e que os endereços eletrônicos utilizados para troca de informações não sejam e-mails de terceiros;
- Sejam solicitados apenas os dados pessoais e documentos comprobatórios mínimos para a realização da operação em andamento, inclusive para fins de realização de novas adesões;
- Não haja a disponibilização de dados pessoais de maiores de 18 anos para terceiros, ainda que pais ou familiares.

6. RESPONSABILIDADES

6.1. Da Diretoria Executiva

- Prover a estrutura para o necessário comprometimento dos colaboradores e para o cumprimento desta Política;

- Garantir a disponibilidade de recursos;
- Dirimir sobre casos não previstos nesta Política.

6.2. Da Gerência de Tecnologia da Informação

- Conduzir análises críticas com a Diretoria Executiva para a manutenção de adequação desta Política;
- Providenciar qualquer alteração pertinente;
- Compartilhar com a Gerência de Governança as ocorrências de descumprimento desta Políticas, visando o estabelecimento de ações de verificação de conformidade.

6.3. Da Gerência de Governança, Riscos e Compliance

- Manter a Política disponível a toda a Braslight;
- Apoiar a Diretoria Executiva, gestores, colaboradores e estagiários no entendimento e aplicação desta Política.
- Analisar ocorrências relatadas a fim de verificar a aderência dos procedimentos estabelecidos nesta Política, compartilhando se necessário com a Diretoria Executiva.

6.4. Da Gerência de Gestão de Pessoas

- Dar conhecimento aos diretores, colaboradores e estagiários sobre a existência desta Política.

6.5. Da Gerência Jurídica

- Apoiar na interpretação da lei e suas modificações que venham impactar nesta Política.
- Identificar fragilidades na adequação à lei, promovendo discussões sobre os ajustes necessários.

6.6. Do(a) *Data Protection Officer*

- Receber do agente de tratamento dos dados todas as informações que identifiquem eventual atividade de tratamento de dados.
- Entender todo o ciclo de vida dos dados pessoais, instruindo o responsável pelo tratamento para que as atividades relacionadas estejam em conformidade com os princípios, direitos e demais exigências que constam da LGPD.
- Levar ao conhecimento dos mais altos escalões hierárquicos do agente de tratamento todas as conclusões e instruções sobre os riscos envolvidos em caso de inadequação com a LGPD.

- Ser o elo entre a organização, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados, atuando como canal de interlocução com estes entes, devendo zelar para que o acesso a ele seja facilitado, de forma gratuita, clara e pública nos meios de comunicação do agente de tratamento.

6.7. Das demais gerências e colaboradores

- Estar comprometido em satisfazer os procedimentos estabelecidos nesta Política;
- Tomar conhecimento das atualizações da Política;
- Zelar pelo cumprimento da Política estabelecida pela Diretoria Executiva.

7. ANEXOS

Não aplicável.

Esta política deverá ser divulgada de forma ampla a todos os colaboradores da entidade e deverá ser revisada a cada dois anos ou sempre que se fizer necessário.

A presente Política foi aprovada em reunião de Diretoria Executiva realizada em 26/10/2021, entrando em vigor a partir dessa data.

Assinado digitalmente por LUCIANO MOLTER DE PINHO GROSSO: 02163018741
Razão: Aprovo
Data: 2021-11-22 10:24:31

Luciano Molter de Pinho Grosso
Diretor Presidente

SUMÁRIO DE REVISÕES		
Versão	**Data**	**Descrição e/ou itens alterados**
1	06/08/2019	Emissão original POL BP-0005/2019.
2	26/10/2021	Revoga-se a POL BP-0005/2019 de 06/08/2019.