

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA PBH ATIVOS

INSTRUÇÃO NORMATIVA N° 002/2021

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA PBH ATIVOS

INSTRUÇÃO NORMATIVA Nº 002/2021

A Diretoria Geral da PBH Ativos S.A., no uso da competência que lhe é atribuída e considerando:

- a) a Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- b) a Lei Federal nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet;
- c) a Lei Federal nº 13.303, de 30 de junho de 2016 - Lei de Responsabilidade das Estatais;
- d) a Lei Federal nº 6.404, de 15 de dezembro de 1976 – Lei das Sociedades Anônimas;
- e) a Lei Municipal nº 10.003, de 25 de novembro de 2010;
- f) as Políticas de Governança da Companhia, em especial, o Código de Conduta Ética e Integridade, a Política de Gestão de Riscos, a Política de Integridade e Anticorrupção e a Política de Classificação de Informações;
- g) a publicação pela Autoridade Nacional de Proteção de Dados do “Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado” em 27 de maio de 2021;
- h) a aprovação pela Diretoria Geral na reunião datada de 17 de agosto de 2021; e
- i) a aprovação pelo Conselho de Administração na reunião datada de 25 de agosto de 2021;

Resolve:

Art. 1º. Expedir a Revisão 001/2021 da Política de Proteção de Dados Pessoais da PBH Ativos S.A., aprovada pela Diretoria Geral e pelo Conselho de Administração, conforme Anexo Único desta Instrução Normativa.

Art. 2º. Fica revogada a Instrução Normativa nº 008/2020.

Art. 3º. Esta Instrução Normativa entra em vigor a partir da data de sua divulgação.

Belo Horizonte, 25 de agosto 2021.

Pedro Meneguetti

Diretor Presidente

Soraya de Fátima M. M. Lage

Diretora Executiva

Daniel Rodrigues Nogueira

Diretor de Negócios

ANEXO ÚNICO

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DA PBH ATIVOS S.A.

1. OBJETIVO

A presente Política busca demonstrar o compromisso da PBH Ativos S.A. (ora denominada “Companhia”) em atuar com atenção às disposições legais e regulamentares pertinentes ao tratamento de dados pessoais, especialmente as previstas na Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), estabelecendo princípios e orientações gerais que devem reger o tratamento de dados pessoais dentro de seu ambiente corporativo, com vistas a:

1.1 estar em conformidade com as leis e regulamentações aplicáveis ao tratamento de dados pessoais e seguir as melhores práticas;

1.2 proteger os direitos de todos os que se relacionam com a Companhia, inclusive empregados e administradores, contra os riscos de violações de dados pessoais e;

1.3 promover a conscientização em toda a Companhia acerca dos principais aspectos que envolvem o tratamento e a proteção de dados pessoais.

2. PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS

Para atender aos padrões de proteção de dados pessoais estabelecidos na legislação e demais regulamentação aplicáveis, o tratamento de dados pessoais no âmbito da Companhia deve observar os seguintes princípios:

2.1 *Princípios da Finalidade e da Adequação*

A Companhia deve garantir que o tratamento de dados pessoais possua propósitos legítimos, específicos, explícitos e informados ao titular, não podendo, posteriormente, ser realizado de forma incompatível com essas finalidades. Deve haver compatibilidade entre o tratamento realizado e as finalidades informadas ao titular no contexto de sua obtenção.

2.2 Princípio da Necessidade

A Companhia deve limitar o tratamento de dados pessoais ao mínimo necessário para atingir suas finalidades. A abrangência dos dados pessoais deve ser pertinente, proporcional e não excessiva em relação às finalidades do tratamento.

2.3 Princípio do Livre Acesso

A Companhia deve garantir aos titulares dos dados pessoais consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

2.4 Princípios da Qualidade dos Dados e da Transparência

A Companhia deve adotar medidas razoáveis para assegurar clareza, exatidão, relevância e atualização dos dados pessoais, de acordo com a necessidade e em relação às finalidades para as quais foram coletados. Busca-se garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os sigilos legais.

2.5 Princípios da Segurança e da Prevenção

A Companhia deve assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos dados pessoais para protegê-los contra o tratamento não autorizado ou ilegal, bem como contra a perda acidental ou destruição ilícita. Tais medidas devem, ainda, prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, que deve garantir a devida confidencialidade.

2.6 Princípio da Não Discriminação

A Companhia deve assegurar que dados pessoais não sejam tratados para fins discriminatórios ilícitos ou abusivos.

2.7 Princípios da Responsabilização e da Prestação de Contas

A Companhia, por meio de seus agentes, deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como a eficácia dessas medidas.

3. HIPÓTESES DE TRATAMENTO E DIREITOS DOS TITULARES

No exercício de suas atividades, para o fiel cumprimento do disposto na Lei Geral de Proteção de Dados Pessoais, a Companhia deve assegurar que somente trata dados pessoais quando o propósito/finalidade do tratamento se enquadra em uma das hipóteses legais nela previstas, devendo, ainda, garantir que os direitos dos titulares dos dados pessoais sejam observados.

3.1 Principais hipóteses legais que autorizam o tratamento de dados pessoais no âmbito Companhia

3.1.1 consentimento do titular dos dados pessoais. Ocorre quando o tratamento de dados pessoais não se enquadra em nenhuma das demais hipóteses legais que dispensam o consentimento. Nesse caso, a Companhia deve assegurar que este consentimento seja obtido de forma específica, livre e inequívoca. Além disso, a Companhia deve coletar, armazenar e gerenciar todas as respostas de consentimento de maneira organizada e acessível, para que a comprovação de consentimento possa ser fornecida quando necessário;

3.1.2 cumprimento de exigência decorrente de lei ou regulamento ao qual a Companhia está sujeita;

3.1.3 celebração e execução de contrato ou de procedimentos preliminares relacionados a contrato, do qual seja parte o titular dos dados pessoais. Nesse caso, a Companhia deve assegurar que as hipóteses de tratamento de dados pessoais estejam previstas no contrato;

3.1.4 exercício regular de direitos do titular dos dados pessoais em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas;

3.1.5 proteção à vida ou à incolumidade física do titular dos dados pessoais ou de terceiros; e

3.1.6 interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Nesse caso, o interesse legítimo deverá ser comunicado previamente ao titular dos dados pessoais.

3.2 Direitos dos titulares de dados pessoais

A Companhia deve se comprometer com a garantia dos direitos dos titulares de dados pessoais, dispostos na Lei Geral de Proteção de Dados Pessoais, os quais se destacam, além daqueles decorrentes dos princípios elencados:

- 3.2.1 direito à informação, quando do fornecimento dos dados pessoais, sobre como serão tratados;
- 3.2.2 direito à informação sobre o tratamento dos dados pessoais e ao acesso aos dados pessoais que a Companhia detenha sobre eles;
- 3.2.3 direito à correção de seus dados pessoais se estiverem imprecisos, incorretos ou incompletos;
- 3.2.4 direito à exclusão, bloqueio e/ou anonimização de seus dados pessoais em determinadas circunstâncias. Isso pode incluir, mas não se limita a, circunstâncias nas quais não seja mais necessário que a Companhia retenha os dados pessoais para os propósitos para os quais foram coletados;
- 3.2.5 direito à restrição do tratamento de seus dados pessoais em determinadas circunstâncias;
- 3.2.6 direito a se opor ao tratamento, se este for baseado em legítimo interesse;
- 3.2.7 direito a retirar o consentimento a qualquer momento, se o tratamento dos dados pessoais se basear no Consentimento do indivíduo para um propósito específico; e
- 3.2.8 direito à revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

4. IMPLEMENTAÇÃO, ATRIBUIÇÕES E RESPONSABILIDADES

A Companhia é responsável pela implementação das diretrizes e dos preceitos previstos na Lei Geral de Proteção de Dados Pessoais, bem como por demonstrar o cumprimento desta Política, devendo promover a adequação e o gerenciamento de suas atividades, conforme as seguintes atribuições e responsabilidades.

4.1 Agentes de tratamento: controlador e operadores

4.1.1 Controlador

A Companhia, nas atividades em que assume papel de controlador de dados, deverá atuar com atenção aos dispositivos previstos na Lei Geral de Proteção de Dados, responsabilizando-se, em especial por:

- a) instruir o operador acerca do tratamento de dados pessoais;
- b) manter os registros das operações de tratamento realizadas;
- c) atender às determinações da Autoridade Nacional de Proteção de Dados (ANPD);
- d) indicar o Encarregado (PDO);
- e) assegurar a observância dos direitos do titular de dados pessoais no âmbito da Companhia.

4.1.2 Operadores

A Companhia, nas atividades em que assume papel de operador de dados, deverá atuar com atenção aos dispositivos previstos na Lei Geral de Proteção de Dados, responsabilizando-se, em especial por:

- a) realizar o tratamento de dados pessoais em conformidade com o instruído pelo Controlador;
- b) realizar e manter os registros das operações de tratamento de dados pessoais no âmbito da Companhia, que deve contar com todos os requisitos previstos na lei.

4.2 Encarregado (DPO)

O Encarregado (DPO) é designado por Portaria pela Diretoria Geral e deve atuar com atenção aos dispositivos previstos na Lei Geral de Proteção de Dados, responsabilizando-se, em especial por:

- a) realizar a interlocução entre os titulares de dados pessoais, a autoridade nacional e a Companhia, recebendo reclamações, comunicações e adotando as providências necessárias; e
- b) orientar ao público interno e demais colaboradores da Companhia a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

4.3 Administradores, empregados e colaboradores da Companhia

4.3.1 Todos os administradores, empregados e colaboradores da Companhia são responsáveis por conhecer e compreender a presente Política de Proteção de Dados Pessoais e devem atuar com atenção aos dispositivos previstos na Lei Geral de Proteção de Dados, responsabilizando-se, em especial por:

- a) usar adequadamente os dados pessoais em suas atividades;
- b) participar de atividades de treinamento em proteção de dados pessoais quando recomendado;

c) relatar para o Encarregado (DPO) a ocorrência de quaisquer incidentes de dados pessoais ou segurança de dados, bem como as deficiências identificadas relacionadas ou possíveis riscos de privacidade.

4.3.2 O descumprimento desta Política poderá resultar em processo administrativo disciplinar, nos termos do Código de Conduta Ética e Integridade da Companhia.

6. DISPOSIÇÕES FINAIS

6.1 Aqueles que tiverem perguntas ou dúvidas a respeito desta Política, devem procurar o Encarregado (DPO) nomeado pela Companhia.

6.2 Nenhuma regra prevista nesta Política proibirá que integrantes ou terceiros reportem preocupações ou atividades ilegais às autoridades competentes.

6.3 A presente Política poderá ser alterada pela Companhia em qualquer momento que for considerado conveniente.

6.4 Qualquer alteração ou revisão da presente Política deverá ser submetida à Diretoria Geral e ao Conselho de Administração.

6.5 Os casos omissos serão decididos pela Diretoria Geral, após manifestação do Encarregado (DPO).

ANEXO I DA POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

GLOSSÁRIO LGPD - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Este glossário visa facilitar o entendimento dos principais termos da Lei Geral de Proteção de Dados Pessoais - LGPD, Lei nº 13.709/18, aprovada em 14 de agosto de 2018. Foi elaborado tendo como fonte a própria Lei, além de orientações disponíveis na Cartilha do Município de Belo Horizonte sobre a Lei Geral de Proteção de Dados Pessoais¹.

“Agentes de tratamento”: o controlador e o operador.

“Anonimização”: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

“Autoridade Nacional”: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

“Banco de dados”: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

“Bloqueio”: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

“Companhia”: Refere-se à PBH Ativos S.A.

“Consentimento”: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Se elaborado de uma forma muito genérica, sem especificação, poderá ser considerado nulo. O consentimento pode ser revogado pelo titular. Quando tratar dados pessoais for condição para fornecimento de produto ou serviço ou para exercício de um direito, você deve ser avisado sobre isso e sobre os meios pelos quais pode exercer seus direitos como titular. A administração pública poderá tratar e compartilhar os dados

¹ Disponível em: <https://prefeitura.pbh.gov.br/sutransp/LGPD>



necessários à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, independentemente do consentimento do titular dos dados, desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

“**Controlador**”: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

“**Criptografia**”: arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem.

“**Dado anonimizado**”: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

“**Dado pessoal**”: informação relacionada à privacidade de uma pessoa natural identificada ou identificável. Alguns exemplos de dados pessoais são: nome, endereço, e-mail, idade, números de documentos de identificação (RG, CPF, CNH, título de eleitor), estado civil, informações relativas à localização geográfica, número de IP, dentre outros.

“**Dado pessoal de criança e de adolescente**”: o Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. Deverá ser coletado o consentimento dos pais ou responsáveis para efetuar tratamento de dados de criança ou adolescente.

“Dado pessoal sensível”: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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. Diz respeito à intimidade de um indivíduo. Merecem proteção especial, uma vez que pode ser usado para fins de discriminação.

“Documentação(ões) Orientadora(s)”: Documento(s) formal(is) da PBH Ativos S.A. que fornece(m) conteúdo sobre decisões, regras e orientações corporativas que são vitais para direcionar o trabalho da Companhia com legitimidade, rastreabilidade e aplicabilidade e deve ser observado e praticado por um certo universo definido de integrantes.

“Eliminação”: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

“Encarregado”: também denominado como Data Protection Officer (DPO), o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

“Garantia da segurança da informação”: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação.

“Garantia da segurança de dados”: ver garantia da segurança da informação.

“Integrante(s)” ou **“Colaborador(es)”**: Funcionários/empregados que trabalham na PBH Ativos S.A. em todos os níveis, incluindo executivos, conselheiros, diretores, estagiários e aprendizes.

“Interoperabilidade”: capacidade de sistemas e organizações operarem entre si, trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente. A autoridade nacional poderá dispor

sobre padrões de interoperabilidade para fins de portabilidade, além dos padrões de interoperabilidade de governo eletrônico (ePING).

“**LGPD**”: Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 da Lei Federal nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet.

“**Operador**”: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

“**Órgão de pesquisa**”: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

“**Política**”: Essa Política de Proteção de Dados da PBH Ativos S.A.

“**Pseudonimização**”: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

“**Relatório de impacto à proteção de dados pessoais**”: documentação emitida pelo controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

“**Titular**”: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

“**Tratamento**”: qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. A meta



visualização de dados por um servidor caracteriza tratamento. Pode ser considerado tratamento toda operação realizada com dados pessoais, como as que se referem a:

- acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer ou eliminar dados;
- armazenamento - ação ou resultado de manter ou conservar em repositório um dado;
- arquivamento - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência;
- avaliação - ato ou efeito de calcular valor sobre um ou mais dados;
- classificação - maneira de ordenar os dados conforme algum critério estabelecido;
- coleta - recolhimento de dados com finalidade específica;
- comunicação - transmitir informações pertinentes a políticas de ação sobre os dados;
- controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados;
- distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- eliminação - ato ou efeito de excluir ou destruir dado do repositório;
- extração - ato de copiar ou retirar dados do repositório em que se encontrava;
- modificação - ato ou efeito de alteração do dado;
- processamento - ato ou efeito de processar dados;
- produção - criação de bens e de serviços a partir do tratamento de dados;
- recepção - ato de receber os dados ao final da transmissão;
- reprodução - cópia de dado preexistente obtido por meio de qualquer processo;
- transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;
- utilização - ato ou efeito do aproveitamento dos dados.

“**Transferência internacional de dados**”: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

“Uso compartilhado de dados”: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

“Vazamento de dados”: transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. Os dados podem ser transferidos eletronicamente ou fisicamente, de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).