POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Código	POL-PP-001	**Versão**	1.0
Aprovação	[●]	**Vigência**	[●]
Responsável	[●]	**Próxima revisão**	[●]
Classificação	Uso Interno	**Área proprietária**	[●]

1. OBJETIVO

Esta Política estabelece princípios, responsabilidades e controles para o tratamento de dados pessoais realizado pelo MEU BENEFÍCIO, no desenvolvimento de suas atividades de administração operacional e comercial de cartões utilizados na modalidade consignada, sem emissão própria, em parceria com instituições emissoras e em convênios com órgãos e entidades públicas.

Esta Política busca assegurar tratamento lícito, legítimo, seguro, transparente e compatível com as finalidades informadas aos titulares, em observância à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), ao Marco Civil da Internet e às demais normas aplicáveis.

2. ABRANGÊNCIA

Aplica-se a administradores, empregados, prestadores de serviços, parceiros comerciais, correspondentes, fornecedores de tecnologia, operadores, suboperadores e demais terceiros que tratem dados pessoais em nome ou no interesse do MEU BENEFÍCIO.

Abrange dados de servidores públicos ativos, aposentados, pensionistas, beneficiários, representantes de órgãos conveniados, usuários de cartões, empregados, candidatos, fornecedores e demais pessoas naturais relacionadas às atividades do MEU BENEFÍCIO.

3. DEFINIÇÕES

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, dado genético ou biométrico vinculado a uma pessoa natural.

Tratamento: toda operação realizada com dados pessoais, incluindo coleta, acesso, uso, transmissão, armazenamento, compartilhamento, eliminação e arquivamento.

Controlador: agente que toma as decisões essenciais sobre as finalidades e os meios do tratamento.

Operador: agente que trata dados pessoais em nome do controlador.

Titular: pessoa natural a quem os dados pessoais se referem.

Incidente de segurança: evento confirmado que comprometa confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.

4. PAPÉIS E RESPONSABILIDADES NO ECOSSISTEMA

A qualificação do MEU BENEFÍCIO como controlador, operador ou controlador conjunta deverá ser definida por operação e refletida nos contratos, fluxos e registros de tratamento.

- A instituição emissora e/ou bancarizadora serão responsáveis pelas decisões regulatórias e creditícias que lhe competirem, inclusive emissão, autorização de transações, gestão da conta ou instrumento de pagamento, faturamento, cobrança e reporte regulatório, conforme o modelo contratado.
- O MEU BENEFÍCIO poderá atuar como controlador independente quanto a cadastros de parceiros, prevenção a fraudes sob sua responsabilidade, gestão de canais próprios, *marketing* próprio, segurança de seus ambientes e cumprimento de obrigações legais próprias.
- O MEU BENEFÍCIO poderá atuar como operador quando tratar dados segundo instruções documentadas da instituição emissora e/ou bancarizadora ou do órgão conveniado.
- Os órgãos e entidades públicas conveniados permanecem responsáveis pelos tratamentos realizados no exercício de suas competências legais, inclusive gestão funcional, folha, margem consignável e autorização de desconto.
- Nenhum contrato poderá atribuir genericamente todos os tratamentos a uma única parte sem considerar quem efetivamente decide cada finalidade e meio essencial.

5. PRINCÍPIOS

- finalidade, adequação e necessidade;
- livre acesso, qualidade dos dados e transparência;
- segurança, prevenção e responsabilização;
- não discriminação;
- privacidade desde a concepção e por padrão;
- limitação de acesso segundo a necessidade funcional.

6. CATEGORIAS DE DADOS TRATADOS

- dados cadastrais e de contato: nome, CPF, data de nascimento, matrícula funcional, endereço, telefone e e-mail;

- dados funcionais e previdenciários: órgão de vínculo, cargo, situação funcional, benefício e informações necessárias à elegibilidade;
- dados financeiros e consignáveis: remuneração, margem disponível, descontos, dados bancários e histórico da operação, quando estritamente necessário;
- dados de contratação e uso: propostas, termos de adesão, gravações, *logs*, aceite eletrônico, faturas, compras, saques, contestações e atendimento;
- dados de autenticação e prevenção a fraudes: documento de identificação, prova de vida, geolocalização aproximada, endereço IP, dispositivo e biometria, quando aplicável;
- dados de representantes, fornecedores, empregados e candidatos.

7. FINALIDADES E BASES LEGAIS

Os dados pessoais poderão ser tratados para as finalidades abaixo, conforme a base legal aplicável e documentada no registro das operações de tratamento:

- cadastro, identificação, autenticação e formalização de adesão ou contratação;
- consulta e gestão de margem consignável, averbação, desconto e conciliação com órgãos conveniados;
- execução dos serviços contratados com a instituição emissora e/ou bancarizadora e demais parceiros;
- prevenção a fraude, segurança, gestão de risco, auditoria e investigação interna;
- atendimento, ouvidoria, contestação, exercício de direitos e solução de reclamações;
- cumprimento de obrigação legal ou regulatória e exercício regular de direitos;
- proteção do crédito e cobrança, quando cabível;
- *marketing* e comunicação institucional, respeitados consentimento ou legítimo interesse, *opt-out* e avaliação de impacto quando necessários;
- recrutamento, gestão de pessoas e contratação de fornecedores.

O consentimento não será utilizado como base genérica para tratamentos necessários à execução contratual, ao cumprimento de obrigação legal, à prevenção de fraude ou ao exercício regular de direitos.

8. DADOS BIOMÉTRICOS

O tratamento de biometria somente ocorrerá quando necessário para autenticação, prevenção a fraude, segurança do titular ou formalização eletrônica, com base legal adequada, controles reforçados e avaliação prévia de proporcionalidade.

- armazenamento preferencial de *templates* biométricos ou evidências criptográficas, evitando imagens brutas quando desnecessárias;
- segregação de acesso e criptografia;
- prazo de retenção definido;
- vedação de reutilização para finalidade incompatível;

- auditoria de fornecedores de biometria e prova de vida.

9. COMPARTILHAMENTO DE DADOS

O compartilhamento poderá ocorrer com instituições emissoras, bancarizadora, processadoras, bandeiras, fornecedores de tecnologia, antifraude, assinatura eletrônica, atendimento, cobrança, auditoria, órgãos públicos conveniados, autoridades e demais terceiros necessários à operação.

Todo compartilhamento deverá observar necessidade, finalidade, base legal, segurança, confidencialidade, minimização e instrumento contratual adequado. **É vedada a venda de dados pessoais.**

10. DIREITOS DOS TITULARES

- confirmação da existência de tratamento e acesso;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade;
- portabilidade, quando regulamentada e aplicável;
- informação sobre compartilhamentos;
- revogação do consentimento e oposição, quando cabíveis;
- revisão de decisões tomadas unicamente com base em tratamento automatizado, nos termos legais.

As solicitações deverão ser encaminhadas pelo canal de privacidade [•]. A identidade do solicitante deverá ser validada de forma proporcional ao risco. Pedidos que envolvam tratamentos realizados por outro controlador serão direcionados à parte competente, sem prejuízo do apoio do MEU BENEFÍCIO.

11. RETENÇÃO E ELIMINAÇÃO

Os dados serão mantidos pelo prazo necessário às finalidades, aos contratos, às obrigações legais, regulatórias e de auditoria, à prevenção a fraude e ao exercício regular de direitos. Encerrado o prazo, serão eliminados, anonimizados ou arquivados com acesso restrito, conforme tabela corporativa de temporalidade.

12. SEGURANÇA DA INFORMAÇÃO

- controle de acesso baseado em função e privilégio mínimo;
- autenticação multifator para acessos críticos;
- criptografia em trânsito e, quando aplicável, em repouso;
- gestão de vulnerabilidades, *logs*, *backups* e continuidade de negócios;
- segregação de ambientes e testes periódicos;
- avaliação de fornecedores e cláusulas de segurança e privacidade;

- treinamento periódico e compromisso de confidencialidade.

13. INCIDENTES DE SEGURANÇA

Todo incidente ou suspeita deverá ser comunicado imediatamente ao Encarregado e à área de Segurança da Informação. O MEU BENEFÍCIO manterá procedimento de resposta com contenção, preservação de evidências, avaliação de risco, comunicação às partes controladoras e, quando aplicável, à ANPD e aos titulares, nos prazos e condições legais.

14. GOVERNANÇA E RESPONSABILIDADES

- Conselho de Administração/Diretoria: aprovar a Política e assegurar recursos.
- Encarregado: orientar, receber comunicações, acompanhar conformidade e atuar como canal com titulares e ANPD.
- Jurídico/*Compliance*: avaliar bases legais, contratos, riscos e mudanças normativas.
- Tecnologia e Segurança: implementar medidas técnicas e responder a incidentes.
- Áreas de negócio: observar minimização, finalidade e registros de tratamento.
- Terceiros: cumprir as instruções, medidas e obrigações contratadas.

A Diretoria aprovará esta Política e designará o Encarregado de Dados.

15. PRIVACIDADE DESDE A CONCEPÇÃO (PRIVACY BY DESIGN)

Novos produtos, convênios, integrações e contratação de fornecedores que envolvam dados pessoais deverão passar por avaliação prévia de privacidade e segurança. Relatório de Impacto à Proteção de Dados será elaborado quando o tratamento puder gerar alto risco aos titulares, especialmente em biometria, perfilamento, decisões automatizadas ou tratamento em larga escala.

16. TREINAMENTO, MONITORAMENTO E SANÇÕES

O MEU BENEFÍCIO promoverá treinamento periódico e monitorará a aderência a esta Política. Violações poderão resultar em medidas disciplinares, rescisão contratual, responsabilização civil, administrativa e criminal, sem prejuízo da comunicação às autoridades competentes.

17. REFERÊNCIAS

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.
- Lei nº 12.965/2014 – Marco Civil da Internet.
- Normas, regulamentos e orientações vigentes da Autoridade Nacional de Proteção de Dados.
- Contratos com instituições emissoras e/ou bancarizadora, órgãos conveniados e fornecedores.

18. DISPOSIÇÕES FINAIS

Esta Política deverá ser revista, no mínimo, a cada 01 (um) ano ou sempre que houver alteração relevante no modelo de negócio, nos riscos, nas tecnologias empregadas ou na legislação aplicável.

APROVAÇÃO E REVISÃO

Nome	Cargo	Assinatura	Data
[●]	[●]	[●]	[●]