1. Objetivo: Esta política tem como objetivo estabelecer as diretrizes para a coleta, armazenamento, uso, compartilhamento e eliminação de dados pessoais tratados pela Primova e suas empresas associadas, garantindo conformidade com a legislação aplicável e promovendo a segurança, transparência e privacidade no tratamento de dados.

2. Abrangência: esta política se aplica a todos os colaboradores, fornecedores, parceiros, prestadores de serviço e demais terceiros que possuam vínculo com o Grupo Primova, abrangendo, subsidiárias, coligadas e associadas, independentemente de sua posição hierárquica ou local de atuação.

3. Diretrizes Gerais

- Garantir a proteção e privacidade dos dados pessoais coletados e tratados;
- Assegurar conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e demais normas aplicáveis;
- Promover a transparência no tratamento de dados pessoais;
- Aplicar medidas de segurança e controle de acesso para evitar incidentes de segurança;
- Definir responsabilidades e obrigações dos envolvidos no tratamento de dados pessoais;
- Facilitar o exercício dos direitos dos titulares de dados;
- Implementar políticas internas de segurança e confidencialidade das informações;
- Monitorar e auditar periodicamente o cumprimento das diretrizes estabelecidas nesta política.

4. Normas Aplicáveis Esta Política está em conformidade com:

- Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018);
- Marco Civil da Internet (Lei nº 12.965/2014);
- Código de Defesa do Consumidor (Lei nº 8.078/1990);
- Regulamento Geral de Proteção de Dados (GDPR) - quando aplicável;
- Normas e diretrizes da Autoridade Nacional de Proteção de Dados (ANPD);
- Demais regulamentações aplicáveis ao tratamento de dados pessoais.

5. Princípios do Tratamento de Dados

- Finalidade: tratamento para propósitos legítimos, específicos e informados;
- Adequação: compatibilidade com as finalidades declaradas;
- Necessidade: limitação à coleta e tratamento do mínimo necessário;
- Livre Acesso: garantia de consulta facilitada aos titulares;
- Segurança: adoção de medidas para evitar acessos indevidos;
- Transparência: comunicação clara e acessível sobre o tratamento de dados;
- Prevenção: adoção de medidas para evitar incidentes de segurança;
- Não Discriminação: vedação de tratamento para fins discriminatórios ilícitos;
- Responsabilização: comprovação da adoção de medidas eficazes de proteção.

6. Quanto à Informação

- Toda informação deve ser utilizada apenas para fins profissionais;
- Não é permitida a divulgação de informações sigilosas sem autorização;
- Informações devem ser protegidas contra acesso, modificação ou destruição não autorizada;
- Recursos tecnológicos devem ser utilizados de forma autorizada e segura;
- As informações devem ser armazenadas pelo tempo determinado pela organização ou legislação vigente;
- A recuperação de informações deve ocorrer somente quando necessário e com autorização expressa do proprietário;
- A geração, uso, armazenamento, manutenção e descarte de informações devem seguir as necessidades da empresa e a legislação aplicável;
- Equipamentos e instalações da empresa são ferramentas de trabalho e seu uso pode ser monitorado, inspecionado ou auditado sempre que necessário, observando-se os preceitos legais.

7. Quanto aos Colaboradores

- Devem seguir integralmente as diretrizes da Política de Segurança e Privacidade;
- Devem manter-se atualizados quanto às normas internas e legislações aplicáveis;
- Não podem divulgar informações da empresa sem autorização formal;
- Não podem usar sistemas internos para intimidação, assédio ou violação de privacidade;
- O uso de senhas e acessos deve ser pessoal e intransferível;
- Devem adotar boas práticas no uso dos recursos tecnológicos da empresa;
- Devem garantir que informações não sejam compartilhadas de forma inadequada;
- Devem respeitar normas de controle de acesso e diretrizes de privacidade da empresa.

8. Quanto ao Ambiente

- Medidas devem ser adotadas para investigar e mitigar incidentes de segurança;
- A segurança física e do ambiente deve ser mantida para proteger dados e informações;
- A empresa se reserva o direito de monitorar, auditar e intervir em acessos de dados conforme necessário para salvaguardar seus interesses;
- Equipamentos e redes corporativas devem ser utilizados apenas para fins profissionais.

9. Controles e Normas

- Gestão de Recursos Humanos: Informar prontamente desligamentos, afastamentos e modificações no quadro funcional;
- Gestão Administrativa: Garantir a confidencialidade de informações estratégicas acessadas por terceiros;
- Controles de Acesso: Definir e monitorar permissões de acesso conforme a necessidade.

10. Segurança da Informação

- Monitoramento contínuo para identificação de riscos;

- Implementação de medidas para evitar vazamento de dados;
- Proteção contra ataques cibernéticos e acessos indevidos;
- Treinamento e conscientização dos colaboradores sobre proteção de dados;
- Manutenção de um plano de resposta a incidentes de segurança;
- Aplicação de controles para garantir a confidencialidade, integridade e disponibilidade das informações.

11. Direitos dos Titulares Os titulares podem solicitar:

- Confirmação do tratamento de seus dados;
- Acesso aos dados armazenados;
- Correção de informações incorretas;
- Exclusão de dados tratados sem base legal;
- Portabilidade dos dados a outro fornecedor;
- Revogação do consentimento quando aplicável.

12. Encarregado de Proteção de Dados (DPO)

- Receber comunicações e reclamações de titulares;
- Atender solicitações da ANPD;
- Monitorar a conformidade da empresa com as normas de privacidade;
- Promover treinamentos e atualização contínua sobre proteção de dados;
- Executar ações conforme diretrizes da empresa e requisitos regulatórios.

13. Contato e Relato de Incidentes Em caso de dúvidas ou para relatar incidentes de segurança, entre em contato com o DPO pelo e-mail: [inserir e-mail do DPO].