POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS - SALINA DIAMANTE BRANCO

SUMÁRIO

I. INTRODUÇÃO.

Com o aumento exponencial da utilização de dados pessoais tanto pelo setor privado como pelos órgãos públicos, surgiu a necessidade de uma maior proteção e garantia de direitos fundamentais como o da privacidade, liberdade e o livre desenvolvimento da personalidade da pessoa natural. É nesse contexto que, em 2018, foi criada a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) cujo objetivo principal é regular a proteção de dados no Brasil.

Nesse sentido, a LGPD surge como um marco do início de uma nova cultura, que visa a transparência centrada na pessoa física, na minimização do impacto e no aumento da segurança aplicada ao tratamento dos dados pessoais. Em vigor desde 2020, a legislação estabelece a forma como as empresas realizam a coleta, o uso, o armazenamento, o compartilhamento e o controle de dados pessoais em solo nacional.

Os impactos da legislação são diversos, afetando todas as empresas em maior ou menor grau, tendo em vista que a lei atribui uma série de sanções e exigências caso não seja efetivamente cumprida. Para além da questão de cumprimento legal, estar adequado a LGPD garante uma melhoria na gestão, fluxo e estrutura da empresa, bem como um fortalecimento com parceiros de negócios, clientes e uma maior segurança e confiabilidade perante o mercado como um todo, evidenciando a urgência de adaptação ao previsto na lei.

II. CONCEITOS BÁSICOS.

- **DADO PESSOAL:** Informação relacionada à pessoa natural identificada ou identificável. Ex.: nome, CPF, RG, endereço, fotografias, gênero etc.

- **TITULAR DO DADO:** O indivíduo a quem os dados se referem, ou seja, o proprietário dos dados pessoais.

- **DADO PESSOAL SENSÍVEL:** São dados que revelam informações relacionadas à origem racial ou étnica, convicção religiosa, opinião política, dado referente à

saúde ou à vida sexual, dado genético ou biométrico quando vinculadas a uma pessoa física. Tais dados possuem hipóteses mais restritas de tratamento.

- **DADO ANONIMIZADO:** Dado que se refere a um titular que não pode mais ser identificado, ocorre quando um dado pessoal ou um dado pessoal sensível perde a sua individualidade. Em geral, dados anonimizados são utilizados em estudos estatísticos. Ex. dados genéricos que identifiquem ao indivíduo como pertencente a um determinado grupo (homem, 60 anos, aposentado), mas que não têm capacidade de identificá-lo individualmente

- **CONTROLADOR:** Pessoa física ou jurídica responsável pelas decisões relativas ao tratamento dos dados pessoais. Cabe a ele determinar a finalidade e forma de tratamento dos dados, além de ser o responsável caso haja quaisquer incidentes envolvendo os dados. Ex. uma empresa que coleta dados para empregar funcionários, uma escola que coleta dados de alunos

- **OPERADOR:** Pessoa física ou jurídica que realiza o tratamento dos dados pessoais sob o comando do controlador. Ex. uma assessoria contábil que processa pagamentos de funcionários de várias empresas, um sistema em nuvem que hospeda dados.

- **ENCARREGADO:** Pessoa indicada pelo controlador e operador para intermediar a comunicação entre o controlador, os titulares de dados, e a Autoridade Nacional de Proteção de Dados (ANPD). Também chamado de Data Protection Officer (DPO).

- **TERCEIRO:** É toda pessoa física ou jurídica contratada pela empresa para desenvolver ou auxiliar no desenvolvimento de suas atividades, tanto na qualidade de fornecedores de bens ou serviços, como de parceiros comerciais.

- **TRATAMENTO:** Qualquer tipo de operação realizada com os dados pessoais de um indivíduo. Exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **CONSENTIMENTO:** É uma manifestação livre, informada e inequívoca pela qual o titular permite o tratamento de seus dados pessoais para uma determinada finalidade.

- **BASE LEGAL:** Uma base legal é uma finalidade prevista em lei para que empresas, entidades e o poder público possam tratar dados pessoais. Ex. a execução de um contrato de trabalho é uma finalidade prevista para coletar dados necessários de funcionários. O consentimento pode ser uma base legal para mandar e-mail marketing. O cumprimento de obrigação legal pode requerer que você guarde alguns dados coletados por um período. Existem 10 bases legais dando permissões diferentes para o uso de dados pessoais.

III. OBJETIVO E APLICAÇÃO.

A presente Política de Privacidade e Proteção de Dados Pessoais tem como objetivo geral fornecer orientações sobre como gerenciar as diversas atividades e operações de tratamento de dados pessoais existentes na Empresa Salina Diamante Branco.

Nesse sentido, o documento visa estabelecer as diretrizes necessárias para orientar a todos os membros da equipe os cuidados a serem observados para a manutenção das Informações, tendo como referência a Lei Geral de Proteção de Dados Pessoais, entre outras normas nacionais e internacionais relativas à privacidade e proteção de dados pessoais.

A política se aplica ***(i)*** aos empregados da SDB; ***(ii)*** a todos os terceiros, sejam eles pessoas físicas ou jurídicas que atuam para ou em nome da SDB em operações que envolvam tratamento de dados pessoais que sejam realizadas no escopo das atividades conduzidas pela SDB; ***(iii)*** aos agentes de tratamento de dados pessoais externos à SDB que de qualquer forma se relacionem com a Instituição; e ***(iv)*** aos titulares de dados pessoais, cujos dados são tratados pela empresa.

Dito isso, é importante destacar que a adesão ao programa de conformidade da Empresa às leis de proteção de dados pessoais e aos diplomas normativos dele decorrentes, incluindo a presente Política, é obrigatória a todos os destinatários acima indicados na medida em que se relacionam à SDB. Todas as operações que envolvam tratamento de dados pessoais que sejam realizadas no escopo das atividades conduzidas pela Salina estão sujeitas a tais normativas.

IV. REGRAS GERAIS.

IV.1. PRINCÍPIOS.

A Salina Diamante Branco deverá respeitar os seguintes princípios de proteção de dados pessoais quando do tratamento de dados pessoais:

- **FINALIDADE**: A Empresa realizará o tratamento de dados pessoais de forma legítima, específica, explícita e informada ao titular. Assim, a SDB deve informar qual a sua intenção ao fazer o uso daqueles dados e como eles serão utilizados, não podendo alterar essa finalidade durante o tratamento;

- **ADEQUAÇÃO:** O tratamento de dados pessoais será realizado de forma compatível com as finalidades informadas ao titular de dados, e de acordo com o contexto do tratamento;

- **NECESSIDADE:** O uso dos dados deve ser pertinente, proporcional e estritamente necessário. Ou seja, a empresa apenas só irá utilizar o que realmente precisa;

- **LIVRE ACESSO**: a Empresa garantirá aos titulares de dados pessoais a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados;

- **QUALIDADE DOS DADOS:** Os dados utilizados no tratamento devem ser exatos, claros, relevantes para a finalidade e corretos. Sendo atualizados conforme a necessidade do contexto ao qual o tratamento está inserido;

- **TRANSPARÊNCIA:** A empresa irá garantir ao titular do dado que ele possua informações claras e precisas a respeito do tratamento ao qual os seus dados passarão;

- **SEGURANÇA**: A empresa utilizará 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**: Sempre adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

- **NÃO DISCRIMINAÇÃO**: Garantir a impossibilidade do uso de dados pessoais, como a de origem racial, crença religiosa ou posicionamento político, para tratamentos com fins discriminatórios e/ou ilícitos;

- **RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS**: Comprometimento para demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, e a eficácia dessas medidas.

IV.2. DEVERES E RESPONSABILIDADES.

Os deveres de cautela, atenção e uso adequado de dados pessoais se estendem a **todos os destinatários desta Política no desenvolvimento** de seus trabalhos e atividades na Salina Diamante Branco, existindo um compromisso de contribuir para que a Empresa cumpra suas obrigações na implementação de sua estratégia de privacidade e proteção de dados pessoais.

É **dever dos titulares dos dados**, comunicarem à SDB sobre quaisquer modificações em seus dados pessoais na sua relação com a Instituição, seja pelo e-mail institucional, de forma presencial a determinado setor ou qualquer outro meio cabível.

Incumbe aos **empregados da SDB, agentes de tratamentos de dados pessoais e terceiros**, obter a autorização necessária para o tratamento de dados e ter os documentos necessários que demonstrem a designação de sua competência para a realização da operação de tratamento de dados pessoais. Ademais, é dever de tais partes não compartilhar e nem garantir acesso aos dados pessoais mantidos pela Empresa para quaisquer pessoas não autorizadas ou competentes de acordo com as normas da Instituição.

IV.3. DATA PROTECTION OFFICER - DPO.

O chamado *Data Protection Officer*, ou encarregado, é a pessoa indicada pelo Controlador (pessoa física ou jurídica responsável por administrar e tomar decisões sobre o tratamento de dados pessoais) para atuar na comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANDP).

Nesse sentido, o DPO é o responsável por efetivar as atividades, documentos e programas relacionados a proteção de dados pessoais na empresa, sendo seu dever:

- Certificar que todas as regras e que a presente política seja colocada em prática por todos os membros da SDB;

- Orientar e se disponibilizar a esclarecer quaisquer dúvidas referente a proteção de dados da empresa;

- Garantir que todos procedam suas atividades em consonância com os princípios listados no item acima;

- Elaborar revisão de documentos e relatórios de impactos com relação a proteção de dados;

- Solucionar eventuais problemas que tratem de segurança de dados, principalmente relacionada a operação de tratamento de dados pessoais realizada sem base legal, em desconformidade com a Política de Segurança da Informação da SDB ou qualquer outra violação desta Política.

IV.4. PROIBIÇÕES.

Visando uma maior segurança da informação e proteção de dados na empresa, é essencial destacar alguns pontos que devem ser proibidos aos funcionários e colaboradores da Empresa Salina Diamante Branco. Vejamos:

- É expressamente proibido o acesso a quaisquer Informações de clientes, colaboradores ou qualquer registro nos sistemas de Informação da SDB sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa;

- É expressamente proibido o acesso a dados de clientes por mera curiosidade;

- É expressamente proibido o envio de Informações classificadas como "internas" e "confidenciais" para endereços de e-mail de outros domínios além da Empresa, exceto para terceiros (clientes ou fornecedores) diretamente envolvidos no respectivo assunto da mensagem;

- Utilizar programas que burlem os controles de segurança e controle impostos pela SDB ou por seus normativos;

- Armazenar arquivos pessoais e/ou não pertinentes ao negócio da SDB (fotos, músicas, vídeos etc.) para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores e acumular dados pessoais não necessário as atividades da Empresa.

IV.5. RISCOS QUE DEVEM SER EVITADOS.

Em geral, os riscos típicos que a presente política de segurança busca evitar são:

- Revelação de informações sensíveis para terceiros não autorizados;
- Revelação de informações pessoais para terceiros não autorizados;
- Modificações indevidas de dados e programas;
- Perda de dados e programas;
- Destruição ou perda de recursos e instalações;
- Roubo/furto de dados pessoais;
- Utilização indevida dos dados coletados;
- Acessos não autorizados.

IV.6. RELAÇÃO COM TERCEIROS.

Analisando a Lei Geral de Proteção de Dados, percebe-se que a responsabilidade no caso de danos patrimoniais, morais, individuais ou coletivos derivados de violações à legislação de proteção de dados pessoais é solidária, ou seja, todos os agentes da cadeia envolvendo o tratamento de dados pessoais podem ser responsabilizados pelos eventuais danos causados.

Por esse motivo, é primordial que sejam efetuados empenho para verificar, avaliar e garantir que tais terceiros cumpram com as legislações de proteção de

dados aplicáveis, tendo em vista a possibilidade de a SDB ser responsabilizada por tais ações.

Diante te tal ponto, todos os contratos com terceiros deverão conter cláusulas tratando sobre à proteção de dados pessoais, estipulando deveres e obrigações envolvendo tal ponto, e garantindo o compromisso dos terceiros com as legislações de proteção de dados pessoais aplicáveis. Ademais, se faz necessário explanar desde do início das negociações, a política de segurança estabelecida pela empresa, fazendo com que o terceiro fique ciente da importância de estar em consonância com a LGPD.

IV.7. SANÇÕES.

Essencial destacar que a Lei Geral de Proteção de Dados estipula uma série de sanções aos agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, ficando sujeitos a algumas sanções administrativas aplicáveis pela autoridade nacional, tais como:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- Multa diária, observado o limite total a que se refere o inciso II;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;

- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Nesse sentido, a violação desta Política poderá acarretar sanções administrativas e/ou legais, sem prejuízo da rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor e/ou sócio.