

## Política Geral de Proteção de Dados Pessoais

Emitido em 29/12/2022 por Apeme – Associação de Pequenas e Médias Empresas de Garibaldi

Classificação: Uso interno

Versão 1.0

### **Finalidade**

A Política de Proteção de Dados Pessoais tem por finalidade estabelecer diretrizes, princípios, objetivos e conceitos a serem seguidos por todas as partes relacionadas com a Apeme – Associação de Pequenas e Médias Empresas de Garibaldi visando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n.º 13.709/2018.

### **Aplicabilidade**

Esta política é aplicável aos diretores, conselheiros, colaboradores, prestadores de serviço, consultores internos e externos e às entidades públicas e/ou privadas que, de alguma forma, se relacionem com a Apeme.

### **Termos e definições – segurança da informação**

1. Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;
2. Dado Pessoal Sensível: dado pessoal 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;
3. Dado Anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
4. Tratamento de dados pessoais: toda operação realizada com dados pessoais, como as que se referem 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;
5. Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
6. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
7. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
8. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
9. Usuário dos dados pessoais: colaboradores, diretores, conselheiros ou terceiros devidamente autorizados a utilizar ou manipular quaisquer dados pessoais na posse da associação para o desempenho de suas atividades;

10. Autoridade Nacional de Proteção de dados: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) em todo território nacional brasileiro;
11. Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
12. Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
13. 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;
14. Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações controladas pela associação;
15. Violação de dados pessoais: situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade.

### **Esta política tem como propósito**

1. Impor a adoção de controles técnicos, jurídicos e organizacionais para o cumprimento das legislações;
2. Assegurar aos titulares de dados pessoais, especialmente aqueles que tem seus dados pessoais tratados pela associação, o direito fundamental à privacidade e ao livre desenvolvimento da personalidade;
3. Regulamentar ações preventivas para possíveis incidentes de violação de dados pessoais e corretivas para a eventualidade de se materializarem;
4. Evitar danos financeiros, reputacionais, de imagem ou qualquer outro impacto negativo relacionado a ausência de conformidade com as legislações antes referenciadas;
5. Consolidar posição da associação como organização mantenedora de sólida estrutura de governança, especialmente em relação ao tratamento de dados pessoais.

### **Tratamento de Incidentes de Violação de Dados Pessoais**

1. Para efeitos desta política, a associação considera um incidente de violação de dados pessoais qualquer ato e ou omissão que possua potencial de quebra da confidencialidade, integridade e disponibilidade de uma informação pessoal, ou seja, uma violação que provoque, de modo acidental ou ilícito, a exposição de dado pessoal, a destruição/perda ou alteração indevida de dado pessoal armazenado ou transmitido, ou o acesso não autorizado por terceiro de uma informação que a ele não se destinava ou não deveria ter sido destinada;
2. É política da associação em relação ao tratamento de incidentes:
  - 2.1. Adotar medidas de segurança, técnicas e administrativas aptas a evitar a ocorrência de violações de dados pessoais;
  - 2.2. Monitorar, identificar e corrigir vulnerabilidades que possam resultar em incidentes;
  - 2.3. Adotar rigor técnico no tratamento dos incidentes identificados;
  - 2.4. Adotar as ações necessárias para abrandar os efeitos decorrentes de eventual incidente;

2.5. Comunicar a autoridade nacional e os titulares quando o incidente puder acarretar risco ou dano relevante aos titulares;

2.6. Observar o prazo razoável definido pela autoridade nacional para a comunicação de incidentes;

2.7. Implementar melhorias contínuas nos processos de identificação, correção e mitigação de incidentes que resultem na violação de dados pessoais.

3. Todas as ações e/ou omissões que caracterizem um incidente de violação de dados pessoais devem ser comunicados imediatamente ao Encarregado pelo Tratamento de Dados Pessoais (DPO), juntamente com as seguintes informações:

3.1. Descrição dos dados pessoais afetados;

3.2. Informações sobre os titulares envolvidos;

3.3. Data e horário que o incidente ocorreu ou foi identificado;

3.4. Quais medidas foram adotadas para reverter ou mitigar os efeitos do incidente.

3.5. O tratamento de incidentes de dados pessoais é classificado como confidencial, sendo vedado o compartilhamento de informações relacionados ao evento com terceiros, inclusive colaboradores cuja o conhecimento a respeito do fato seja dispensável;

6.5. Qualquer comunicado ou reporte sobre o acidente, seja para a imprensa, seja para a Autoridade Nacional de Proteção de Dados, deve ser aprovado pelo Comitê de Compliance e Riscos.

### **Das responsabilidades e sanções**

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, ficam sujeitos a sanções previstas na Lei e Regulamento de Pessoal, desde que seja garantida a ampla defesa e contraditório

### **Disposições finais**

O não cumprimento das diretrizes desta Política poderá ensejar na apuração de responsabilidade aos agentes de tratamento, com base nos normativos internos e legislação em vigor.

Os casos omissos ou as exceções desta Política devem ser submetidas pela Ouvidoria ou pelo Encarregado de Dados ao Controlador que poderá levar à apreciação do Conselho;

Esta Política será revisada a cada 2 (dois) anos ou atualizada sempre que necessário.