CARTILHA DE BOAS PRÁTICAS E DE GOVERNANÇA E PROGRAMA DE PRIVACIDADE DE DADOS.

Câmara Municipal de Araçatuba – Em Conformidade com a LGPD.

O Que é LGPD e Por Que se Aplica a Nós

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) estabelece regras sobre como dados pessoais devem ser coletados, tratados e armazenados, aplicando-se integralmente ao **Setor Público**. O objetivo é proteger a liberdade e a privacidade dos cidadãos.

Conceito	
Dado Pessoal	Qualquer informação que identifique ou possa identificar uma pessoa natural (Ex: nome, CPF, e-mail pessoal, endereço, dados de eleitores, servidores, etc.).
Tratamento	Qualquer operação feita com um dado pessoal: coleta, acesso, uso, modificação, armazenamento, eliminação, etc.
Finalidade Pública	O tratamento de dados deve ser realizado para o atendimento da **finalidade pública** e para a execução das competências legais da Câmara.

II. Princípios Fundamentais e Compliance (Art. 6º da LGPD)

Todo o tratamento de dados pessoais na Câmara deve observar os seguintes princípios, que são a base da conformidade:

- **Finalidade:** Realizar o tratamento apenas para propósitos legítimos, específicos e informados ao titular.
- **Adequação:** O tratamento deve ser compatível com as finalidades informadas.
- **Necessidade:** Usar apenas os dados estritamente necessários para a finalidade, com minimização da coleta.
- **Livre Acesso:** Garantir aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados.
- **Qualidade dos Dados:** Garantir a exatidão, clareza, relevância e atualização dos dados.
- **Transparência:** Garantir informações claras, precisas e facilmente acessíveis sobre o tratamento dos dados.
- **Segurança e Prevenção:** Adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação.
- **Não Discriminação:** Impossibilidade de realizar o tratamento para fins discriminatórios ilícitos ou abusivos.
- **Responsabilização e Prestação de Contas:** Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

III. Governança, Papéis e Documentação (Recomendações TCE-SP).

A. O Papel do Encarregado (DPO)

O Encarregado pelo Tratamento de Dados Pessoais (DPO) é o principal responsável pela LGPD na Câmara:

Função do Encarregado (DPO)	Sua Ação
Orientação	Orientar os colaboradores da Câmara a respeito das práticas relacionadas à proteção de dados pessoais.
Monitoramento	Monitorar a conformidade das atividades de tratamento de dados.
Comunicação	Atuar como canal de comunicação com a Autoridade Nacional de Proteção de Dados (ANPD) e com os titulares dos dados.

B. Registro das Operações de Tratamento (ROT)

O Registro das Operações de Tratamento (ROT) é um documento obrigatório que mapeia o ciclo de vida dos dados pessoais na Câmara:

- **Fundamento Legal:** Para cada dado coletado, deve estar clara a **base legal** utilizada para o tratamento (Art. 7º e 11 da LGPD).
- **Finalidade:** A finalidade do tratamento deve ser registrada, garantindo que o uso é legítimo e necessário.
- **Segurança:** As medidas técnicas de segurança e o tempo de retenção adotados para a proteção do dado pessoal devem ser registrados.

IV. Boas Práticas de Segurança no Dia a Dia

A segurança da informação é responsabilidade de **todos** os funcionários.

Senhas e Acessos

1. **Crie Senhas Fortes e Únicas:** Use senhas longas (mínimo de 12 caracteres), que combinem letras maiúsculas, minúsculas, números e símbolos.
2. **Não Compartilhe Credenciais:** Senhas e credenciais de acesso são pessoais e intransferíveis. O compartilhamento pode gerar responsabilização em caso de incidente de segurança.
3. **Bloqueio de Tela:** Bloqueie o computador ao se ausentar da mesa de trabalho (Utilize o atalho **Windows + L**).
4. **Princípio do Mínimo Privilégio:** Solicite acesso somente aos sistemas e documentos estritamente necessários para o exercício de sua função.

Segurança Digital (E-mails e Navegação)

1. **Cuidado com Phishing:** Não abra e-mails, anexos ou clique em links de remetentes desconhecidos ou suspeitos. Se o e-mail parecer ser de um colega ou fornecedor, mas

o tom ou o pedido for incomum, **confirme a autenticidade por outro canal** (telefone ou nova mensagem) antes de qualquer ação.

2. **Dispositivos de Armazenamento:** Use mídias removíveis (pendrives, HDs externos) fornecidas pela Câmara e evite conectar dispositivos pessoais para transferir dados de trabalho.
3. **Instalação de Software:** Não instale programas não autorizados ou não licenciados nos equipamentos da Câmara.

C. Tratamento e Compartilhamento de Dados

1. **Compartilhamento Interno:** Compartilhe documentos ou planilhas com dados pessoais **apenas** com os setores e servidores que realmente necessitam daquela informação (Princípio da Necessidade).
2. **Confidencialidade em Contratos:** Cláusulas de LGPD devem ser exigidas em contratos com fornecedores e terceiros que tenham acesso a dados pessoais da Câmara, delimitando suas responsabilidades.
3. **Dados de Crianças e Adolescentes:** O tratamento de dados pessoais de crianças deve ser realizado com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou responsável legal.
4. **Descarte Seguro:** A eliminação de dados (em papel ou digitais) deve ser feita de forma segura e permanente, garantindo a não recuperação da informação.
5. **Dados em Papel:** Documentos físicos contendo dados pessoais devem ser armazenados em locais seguros (armários ou gavetas com chave) preferencialmente fora do horário de expediente.

V. Em Caso de Incidente (Vazamento ou Suspeita)

Um **Incidente de Segurança** é qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade dos dados pessoais.

Se você identificar ou suspeitar de um incidente:

1. **Aja Imediatamente:** Se for no computador, desconecte-o da rede (Wi-Fi ou cabo de rede), se possível, para evitar a propagação.
2. **Informe Imediatamente:** Comunique o ocorrido ao seu superior e, principalmente, ao **Departamento de Informática e Tecnologia (DTI)** e ao **Encarregado pelo Tratamento de Dados Pessoais (DPO)** da Câmara.
3. **Não Tente Resolver Sozinho:** A tentativa de resolver o problema sem conhecimento técnico pode agravar o incidente.

Lembre-se: A observância dessas práticas de segurança e privacidade não é apenas uma obrigação legal (LGPD), mas um dever ético de todo servidor público, zelando pelos dados dos cidadãos e pela imagem da Câmara Municipal de Araçatuba.