ANEXO IV
Detalhamento Técnico do Serviço de Adequação e Manutenção à Lei Geral de Proteção de Dados (LGPD)

Este anexo descreve o escopo, a metodologia e as etapas para a completa adequação e manutenção da conformidade da Prefeitura Municipal de Cotiporã à Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018).

1. OBJETIVO GERAL

A presente contratação visa viabilizar a implementação da LGPD por meio de um diagnóstico completo, o estabelecimento de um plano de ação especializado e a efetiva execução das medidas necessárias para atender às determinações da norma, seguindo as boas práticas de proteção de dados, bem como garantir a conformidade contínua e a sustentabilidade da adequação através das atividades recorrentes de manutenção, protegendo os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade dos titulares de dados.

2. PRAZO E FORMA DE EXECUÇÃO DO SERVIÇO DE ADEQUAÇÃO À LGPD

O Serviço de Adequação à Lei Geral de Proteção de Dados (LGPD), referente ao Item 03 do Termo de Referência, será entregue em um período total de 24 (vinte e quatro) meses. Este período será dividido em duas grandes fases de 12 (doze) meses cada:

- **12 (doze) primeiros meses:** Serão dedicados às atividades de DIAGNÓSTICO do cenário atual do Município em relação à LGPD, incluindo o inventário, avaliação, fluxo de dados e identificação de lacunas, conforme detalhado na Etapa 1 (Diagnóstico do Impacto da Lei nº 13.709/2018) da Seção 3.
- **12 (doze) meses subsequentes:** Serão dedicados às atividades de IMPLEMENTAÇÃO das medidas e planos de ação para a adequação à LGPD, abrangendo as demais etapas metodológicas (da Etapa 2 à Etapa 6) da Seção 3.
- Após a conclusão deste período de 24 (vinte e quatro) meses de adequação e implementação, terão início as Atividades Recorrentes de Manutenção da Adequação à LGPD (referente ao Item 3.1 do Termo de Referência), garantindo a conformidade contínua do Município conforme detalhado na Seção 4.

3. METODOLOGIA E ETAPAS DO SERVIÇO DE ADEQUAÇÃO À LGPD

A pretendida contratação será dividida em seis etapas sequenciais, que deverão ser realizadas pela Contratada, abordando a adequação da governança dos dados pessoais no âmbito das operações do Município de Cotiporã.

3.1. 1ª Etapa - Diagnóstico do Impacto da Lei nº 13.709/2018

Esta fase visa identificar o cenário atual do Município em relação à LGPD.

3.1.1. Atividades e Entregáveis:

- Elaboração de documento contendo o inventário, avaliação, fluxo de dados e identificação de lacunas (gaps) nos seguintes âmbitos:
- Sistemas de informação;
- Sistemas de segurança da informação;
- Processos que tratam de dados pessoais;
- Mapeamento dos controladores e operadores de dados;
- Mapeamento dos dispositivos legais que dão suporte à coleta de dados.
- Criação de um mapa de risco detalhado para compreensão dos riscos identificados.
- Proposição de um cronograma para ajustes de procedimentos, sistemas e processos, com as áreas responsáveis.
- Entrega de um Selo de Certificação de Nível de Amadurecimento 1/6 e um atestado de adequação.
- Entrega da primeira versão do Relatório de Impacto à Proteção de Dados (RIPD), contendo a descrição do tratamento, natureza do tratamento, escopo do tratamento, contexto do tratamento, finalidade do tratamento e identificação e avaliação de riscos.

3.1.2. Detalhamento da Fase:

- A Contratada deverá apresentar o Relatório de Conformidade do Município de Cotiporã sobre as Normas, Leis e demais requisitos legais obrigatórios ou considerados "melhores práticas" na gestão dos dados pessoais em seus processos de negócios, procedimentos internos e demais espécies de atividades que envolvam o tratamento de dados pessoais, nos termos da LGPD.
- Identificação dos papéis de controladores de dados, operadores e Encarregado de Dados (DPO), com a colaboração e auxílio das áreas envolvidas.
- Validação do arcabouço jurídico, no tocante às bases legais e consentimentos para coleta de dados pessoais, contratos, legítimo interesse, obrigações públicas e legais, visando definir o escopo de abrangência jurídica com foco na proteção de dados pessoais.
- Orientação quanto à revisão dos contratos envolvendo prestadores de serviços que coletam ou tratam dados pessoais do Município.
- Auxílio na identificação dos pontos de contato onde são obtidos os consentimentos e quais processos precisam solicitar o consentimento.

3.2. 2ª Etapa - Elaboração do Plano de Recepcionamento da LGPD

Esta fase foca na estruturação e planejamento da governança da LGPD no Município.

3.2.1. Atividades e Entregáveis:

- Definição dos papéis do Encarregado de Dados (DPO) e dos membros do Comitê de LGPD.

- Definição de procedimentos para garantir que os detalhes de contato do DPO estejam disponíveis para todos os assuntos de dados.
- Apontamento e documentação dos proprietários dos processos.
- Identificação das funções da própria organização e dos parceiros (Controladores de Dados / Operadores de Dados).
- Realização de avaliações de risco e privacidade para identificar lacunas iniciais.
- Mapeamento dos processos principais que envolvem dados pessoalmente identificáveis.
- Identificação de quais dados pessoais são processados em qual(is) processo(s).
- Verificação do "propósito de processamento" dos dados pessoais para cada processo.
- Determinação e documentação dos fundamentos legais para o processamento.
- Identificação dos operadores de dados envolvidos nos processos.
- Identificação dos meios pelos quais os dados são processados para cada processo.
- Identificação de qualquer subprocessamento onde aplicável.

3.2.2. Detalhamento da Fase:

- A Contratada será responsável por elaborar o plano de recepcionamento da LGPD nos processos do Município de Cotiporã.
- Composição da estrutura de atendimento ao Data Protection Officer, identificando os principais atributos do indivíduo e auxiliando na definição de quem deverá assumir o papel, no âmbito do Município de Cotiporã.
- Elaboração do Diagnóstico de implementação da LGPD no Município de Cotiporã.

3.3. 3ª Etapa - Definição de Procedimentos de Comunicação e Resposta a Incidentes de Segurança Relacionados ao Vazamento de Dados Pessoais

Esta fase estabelece as diretrizes para a comunicação e resposta a incidentes.

3.3.1. Atividades e Entregáveis:

- Descrição da política de privacidade.
- Descrição do aviso de privacidade para o site do Município.
- Geração de aviso de privacidade para e-mails e papelaria.
- Realização de ações de sensibilização dos servidores, expondo as ações realizadas e a responsabilidade de cada um com a proteção de dados e do contribuinte.

3.3.2. Detalhamento da Fase:

- Proposição de definições de procedimentos de comunicação e respostas aos incidentes de segurança relacionados ao vazamento de dados pessoais.
- Apresentação da relação de ações de correção e/ou mitigação destes incidentes.
- Elaboração dos seguintes documentos, que compõem uma lista mínima e que poderá ter itens acrescentados ou eliminados desde que justificados:

- Aviso de privacidade: documento (também publicável no site) que explica como serão processados os dados pessoais de clientes, visitantes do site e outros.
- Aviso de Privacidade do Funcionário: Documento que explica como o Município processará os dados pessoais de seus funcionários.

3.4. 4ª Etapa - Definição dos Procedimentos de Mitigação dos Riscos Levantados nas Etapas 1 e 2

Esta fase visa a análise e a proposição de estratégias para mitigar os riscos identificados.

3.4.1. Atividades e Entregáveis:

- Identificação do impacto e da probabilidade para os riscos levantados nas Etapas 1 e 2.
- Classificação dos riscos conforme impacto e probabilidade identificados.
- Montagem do mapa de riscos e submissão à aprovação do Comitê de Governança de Dados.
- Ajuste do mapa de riscos conforme decisão colegiada do comitê.

3.4.2. Detalhamento da Fase:

- A Contratada deverá realizar a análise dos riscos identificados nas etapas anteriores, com foco na definição de estratégias de mitigação.
- Elaboração de mapa de riscos consolidado, categorizado por áreas e processos.
- Documentação dos procedimentos de mitigação recomendados para cada risco classificado.
- A entrega final desta etapa deverá incluir o Mapa de Riscos Aprovado, com os respectivos planos de mitigação e registro das decisões do comitê.

3.5. 5ª Etapa - Elaboração do Plano de Ação Baseado no Princípio de Pareto (20/80) para Mitigação dos Riscos Encontrados

Esta fase concentra-se na criação de um plano de ação estratégico e priorizado.

3.5.1. Atividades e Entregáveis:

- Montagem de um plano de ação com base no mapa de riscos aprovado pelo comitê.
- Submissão do plano de ação à aprovação do comitê.
- Ajuste do plano de ação conforme determinação do comitê.

3.5.2. Detalhamento da Fase:

- Com base nos riscos priorizados na etapa anterior, a Contratada deverá elaborar um plano de ação estratégico, considerando o princípio de Pareto para maximizar o impacto das ações.
- Detalhamento das ações corretivas, responsáveis, prazos e indicadores de sucesso.
- Submissão do plano ao Comitê de Governança para validação técnica e estratégica.
- Incorporação dos ajustes e recomendações do comitê.

- Formalização do plano como instrumento de gestão da conformidade e segurança da informação.
- A entrega final deverá conter o Plano de Ação Aprovado, com cronograma, responsáveis e metas definidas.

3.6. 6ª Etapa - Implementação do Plano de Ação e Consolidação da Governança

Esta é a fase de execução e formalização final da adequação.

2.6.1. Atividades e Entregáveis:

- Implementação do plano de ação conforme acordado com o comitê.
- Finalização do Relatório de Impacto à Proteção de Dados (RIPD).
- Apresentação do Plano de Continuidade de Negócio.
- Apresentação da Política de Segurança da Informação.
- Apresentação do Plano de Tratamento de Incidentes e Comunicação.
- Apresentação da Política de Retenção e Descarte de Dados de Pessoa Física.
- Emissão do Selo de Certificação de Amadurecimento 6/6, validando a conformidade e maturidade da governança de dados.

2.6.2. Detalhamento da Fase:

- A Contratada deverá executar as ações previstas no plano aprovado, consolidando a governança de dados pessoais no Município.
- O RIPD finalizado deverá incorporar evidências das ações implementadas.
- A entrega final deverá incluir todos os documentos mencionados, devidamente aprovados e registrados.

4. ATIVIDADES RECORRENTES DE MANUTENÇÃO DA ADEQUAÇÃO À LGPD

Após a fase de implantação, a CONTRATADA deverá garantir a conformidade contínua do Município com a Lei nº 13.709/2018, que prevê:
I – Revisão trimestral das políticas de privacidade, termos de uso, políticas de segurança da informação e de retenção e descarte de dados, incorporando ajustes normativos e tecnológicos;
II – Atualização do Relatório de Impacto à Proteção de Dados (RIPD) sempre que houver mudanças significativas nos processos ou sistemas;
III – Monitoramento contínuo dos controles implementados, com indicadores de conformidade e relatórios mensais para o Comitê de Governança de Dados;
IV – Realização de auditorias internas semestrais para validação da maturidade da governança;
V – Gestão dinâmica de riscos: revisão do mapa de riscos e atualização dos planos de mitigação conforme novas ameaças ou vulnerabilidades identificadas;
VI – Treinamento periódico dos servidores e campanhas de conscientização para manutenção da cultura de proteção de dados;

VII – Suporte na gestão das requisições dos titulares (acesso, correção, exclusão, portabilidade), garantindo prazos legais;
VIII – Apoio na comunicação com a Autoridade Nacional de Proteção de Dados (ANPD) em caso de incidentes ou fiscalizações;
IX – Atualização do Plano de Resposta a Incidentes e do Plano de Continuidade de Negócios, com testes anuais de eficácia;
X – Emissão de relatórios anuais de conformidade e evolução de maturidade, com recomendações estratégicas para a alta gestão.

5. REQUISITOS PARA COMPROVAÇÃO DA QUALIFICAÇÃO TÉCNICA DA CONTRATADA E DOS PROFISSIONAIS DESIGNADOS

Para assegurar a qualidade na prestação dos serviços de adequação à LGPD, a Contratada e seus profissionais deverão atender aos seguintes requisitos:

5.1. Qualificação dos Profissionais:

- A equipe técnica mínima deverá ser constituída de um profissional com certificação de Encarregado de Proteção de Dados (DPO - Data Protection Officer), responsável por executar e/ou coordenar os serviços. Serão aceitas as seguintes certificações:
  - EXIN DPO
  - IAPP Certified Information Privacy Professional
  - Certified Information Privacy Manager (CIPM)
  - Certified Information Privacy Professional/Europe (CIPP/E)
  - Certified Information Privacy Technologist (CIPT)
  - BSI Information Security Management Systems Auditor ISO/IEC 27001
  - ISACA's Privacy Certification
  - Certificação da ASSESPRO para LGPD
- Alternativamente, o profissional encarregado poderá demonstrar sua especialização como DPO mediante diploma de pós-graduação em Proteção dos Dados devidamente registrada no MEC.
- O profissional DPO deverá possuir conhecimentos tanto jurídicos quanto de Tecnologia da Informação (TI) e conhecimentos em Mapeamento de Processos.

5.2. Qualificação da Empresa (Selo de Qualidade/Certificação):

- A Contratada deverá comprovar a qualidade e a conformidade de seus serviços de adequação à LGPD por meio da apresentação de Selo de Qualidade ou Marca de Certificação devidamente registrado e aprovado pelo Instituto Nacional da Propriedade Industrial (INPI), nos termos da Lei nº 9.279/1996 (Lei da Propriedade Industrial).
- O Selo de Qualidade ou Marca de Certificação deverá ser pertinente e compatível com o objeto, especificamente no que tange a serviços de:
  - Gestão da proteção de dados;
  - Segurança da informação;
  - Consultoria e assessoria em conformidade e avaliação da conformidade;
  - Análise e processamento de dados;
  - Controle de qualidade de processos ou sistemas;
  - Acreditação e certificação profissional em privacidade e segurança cibernética.

- A Contratada deverá possuir uma metodologia de avaliação de conformidade que estabeleça níveis de maturidade ou abrangência. Para os fins desta licitação, será exigida a comprovação de, no mínimo, o Nível 1 (um) de maturidade ou certificação, conforme a metodologia própria do Selo ou Marca de Certificação da licitante.
- A comprovação dar-se-á mediante a apresentação de cópia autenticada do certificado de registro do Selo de Qualidade ou Marca de Certificação junto ao INPI.
- A licitante deverá apresentar declaração formal atestando que o escopo das atividades e o nível de maturidade abrangidos são diretamente aplicáveis aos serviços de adequação à LGPD objeto desta licitação.

7. METODOLOGIA DE EXECUÇÃO DOS SERVIÇOS

- Todos os produtos deverão ser entregues em formato padrão de mercado editável e serão avaliados pela equipe do Município de Cotiporã.
- A Contratada deverá comunicar formalmente ao Município quaisquer fatores que possam afetar a execução do serviço, impactando prazos, custos ou qualidade.
- Todos os produtos oriundos desta contratação deverão ser elaborados por profissionais devidamente qualificados.
- O dimensionamento da equipe para execução adequada do serviço contratado será de responsabilidade exclusiva da Contratada.
- Será responsabilidade da Contratada a realização do diagnóstico para o tratamento dos dados pessoais, incluindo o auxílio e orientação no mapeamento dos processos e o mapeamento de dados, além da identificação de lacunas.
- A Contratada deverá propor, com base nas melhores práticas de mercado, medidas técnicas para a implantação de novas rotinas e processos para o tratamento de dados pessoais, com enfoque jurídico e em Tecnologia da Informação (TI), visando a mitigação de riscos, e a prevenção e solução de ocorrências.
- A Contratada deverá manter constante contato com todas as áreas envolvidas, propondo alteração e/ou criação de políticas e normas internas para a adequação das rotinas e processos.
- A Contratada deverá implementar sistemática de identificação e combate de incidentes de segurança e vazamento de dados pessoais, bem como treinar e capacitar os colaboradores.
- As atividades que necessitem da participação direta das equipes do Município (levantamentos, reuniões e apresentações) deverão ser executadas presencialmente nas dependências do Município. Demais serviços poderão ser realizados em ambiente da Contratada.