

## TERMO DE REFERÊNCIA

### **Contratação de consultoria especializada para adequação à LGPD, capacitação e apoio continuado**

**Contratante:** Prefeitura Municipal de Tarumã, SP

**Regime de execução:** Serviços contínuos (12 meses)

**Julgamento:** Menor preço global (com estrita aderência técnica ao escopo)

#### **1. Objeto**

Contratação de empresa especializada para conduzir e apoiar a adequação da Administração Municipal à LGPD, incluindo:

- (i) estruturação de governança e do Comitê Gestor de Proteção de Dados;
- (ii) mapeamento e inventário de dados;
- (iii) elaboração e implantação de políticas, normas e POPs;
- (iv) capacitações gerais, setoriais e formações específicas (DPO e TI);
- (v) mentorias semanais com acompanhamento preferencialmente presencial;
- (vi) revisão contratual, apoio a LAI/Portal e assessoramento jurídico temático;
- (vii) preparação de evidências para o TCE-SP (dimensão i-Gov TI/IEG-M);
- (viii) operação do **Canal do Titular** e orientação sobre gestão de incidentes.

#### **2. Justificativa**

- Cumprimento dos arts. 23 a 30, 37, 41, 46 e 50 da LGPD (bases legais para o tratamento pelo poder público, registro das operações, designação do encarregado, segurança e boas práticas).
- Atendimento a demandas de transparência/LAI com proteção de dados, reduzindo riscos de exposição indevida.
- Melhoria de aderência à **dimensão i-Gov TI do IEG-M/TCE-SP**, com produção de **evidências** de conformidade.
- Mitigação de riscos de incidentes e responsabilização administrativa (Res. CD/ANPD nº 18/2024 – dosimetria e sanções), civis e reputacionais.

#### **3. Escopo detalhado (entregas mínimas)**

##### **3.1 Governança e organização**

- Criação e formalização do **Comitê Gestor de Proteção de Dados** (com gabinete, jurídico, TI, administração e áreas estratégicas), com **capacitação dos integrantes** e reuniões semanais de alinhamento.
- Suporte à **nomeação do Encarregado (DPO)**, publicação e comunicação à ANPD, com **formação** do DPO (aprox. 20h em 2 meses, formato híbrido).

### 3.2 Mapeamento e inventário de dados

- Entrevistas com secretarias, levantamento de bancos de dados, identificação de dados sensíveis e finalidades, avaliação de segurança.
- **Inventário** contendo: tipo de dado, finalidade, base legal, compartilhamento, retenção, descarte.

### 3.3 Normas, políticas e POPs

Elaboração/adaptação, com treinamento de uso, de pelo menos:

- Política de Privacidade e Proteção de Dados;
- Política de Segurança da Informação;
- Controle de Acesso;
- Procedimento de Atendimento ao Titular;
- Plano de Gestão de Incidentes e de Crise;
- Termos de Uso/Consentimento (quando cabível);
- **Política de Mesa e Tela Limpa;**
- Política de Descarte/Eliminação de dados;
- Política de Backup e Recuperação;
- Política de uso de apps de mensagens e e-mails corporativos;
- POPs gerais e **POPs específicos** para dados sensíveis (saúde/RH) e de crianças/adolescentes (saúde, educação, assistência social, esportes).

### 3.4 Capacitação e mentoria

- **Treinamento geral LGPD** (toda a Prefeitura): mínimo **4 horas em 2 encontros online e ao vivo**, em **3 turmas**, com **certificação e listas**; **gravação** com acesso por 6 meses.
- **Capacitações setoriais presenciais semanais** (Saúde, Educação, Assistência Social), 2–3h por encontro.
- **Formação do DPO** (≈20h / 2 meses, híbrido) e **treinamento técnico para TI** (segurança e controles de acesso).
- **Mentorias semanais** (preferencialmente presenciais), **≈2h por encontro**, para acompanhamento, dúvidas, atendimento a titulares, apoio na redação de respostas/pareceres.

- **Capacitações e orientações:** formato híbrido, para servidores, nos diversos setores, temas geral e específicos (saúde, educação, RH, etc) com emissão de certificados

### 3.5 LAI, Portal da Transparência e IEG-M

- Consultoria contínua em **LAI** e publicações no **Portal**, para equilibrar transparência e proteção de dados (pareceres e orientações).
- **Apoio específico ao IEG-M/TCE-SP – LGPD**, incluindo **documentos de evidência** para melhoria do índice.

### 3.6 Canal do Titular e governança recorrente

- Implantar e **operar** (com a Prefeitura) o **Canal de Atendimento ao Titular**, com procedimento de gestão e regulamento do setor.

### 3.7 Revisões contratuais e assessoramento jurídico

- **Revisão de minutas** de editais/contratos (incluindo cláusulas LGPD), reuniões presenciais com compras/jurídico.
- **Apoio jurídico especializado** (profissional inscrito na OAB/SP) para temas de privacidade/ANPD, inclusive elaboração de **pareceres** e **estratégias** quando necessário.

## 4. Cronograma macro (12 meses)

A execução deverá observar **encontros semanais, preferencialmente presenciais (1–2x/semana)**, previamente agendados:

- **Fase 1 (Meses 1–2) – Planejamento e Organização:** Comitê, DPO, diagnóstico inicial, análise de contratos, mapeamento preliminar, capacitação geral (3 turmas).
- **Fase 2 (Meses 3–4) – Mapeamento e Inventário:** entrevistas, identificação de dados sensíveis/finalidades, inventário completo e primeiras políticas/POPs.
- **Fase 3 (Meses 5–8) – Implementação:** políticas e POPs (incl. backup, mesa/tela limpa, segurança), treinamento TI e setoriais, Canal do Titular.
- **Fase 4 (Meses 9–11) – Governança, Auditoria e Evidências:** auditorias internas, ajustes, **reuniões semanais de avaliação**, consolidação de evidências pro IEG-M/TCE.
- **Fase 5 (Mês 12) – Encerramento e Hand-over:** relatório final, plano de melhorias e atualização das evidências.

## 5. Entregáveis mínimos

1. **Ato de criação do Comitê** + atas e plano de trabalho.
2. **Ato de nomeação do DPO** + comprovação de comunicação à ANPD + **certificado de formação do DPO**.
3. **Inventário de dados pessoais** por processo/secretaria (tipo, finalidade, base legal, compartilhamento, retenção, descarte).
4. **Pacote de políticas e POPs** listados no item 3.3 (arquivos editáveis).
5. **Plano de Gestão de Incidentes e de Crise; Política de Backup e Recuperação**.
6. **Regulamento e fluxos do Canal do Titular**, formulários e modelos de resposta.
7. **Capacitação geral** (3 turmas), **capacitações setoriais semanais presenciais, treinamento TI e formação DPO híbrido, com listas de presença e certificados + link de gravações (6 meses)**.
8. **Minutas de cláusulas e aditivos LGPD** para licitações/contratos; revisão de editais e contratos (memória de reuniões com compras/jurídico).
9. **Pareceres/estudos** em temas LGPD/LAI/Portal e **IEG-M (evidências)**.
10. **Relatórios mensais de atividades** + aceite formal da contratante.

## 6. Metodologia mínima

- Entrevistas, oficinas e acompanhamento **semanal preferencialmente presencial**; utilização de questionários e dinâmicas para mapeamento; workshops de validação com as áreas; orientação hands-on para implantação de controles.
- Entregas incrementais com **auditoria interna de conformidade** e correções contínuas.
- Emissão de pareceres, relatórios técnicos e indicações de providências
- Suporte presencial e online; encontros habituais previamente agendados

## 7. Requisitos da equipe da contratada

- Coordenador(a) do projeto com experiência comprovada em LGPD setor público.
- **Advogado(a) OAB/SP** para apoio jurídico temático/ANPD.
- Especialista em Segurança da Informação/Governança (apoio a TI/controles).
- Instrutores para treinamentos gerais e setoriais.

## 8. Obrigações da contratada

- Executar com **peçoal qualificado**, boas práticas e **confidencialidade/segredo** das informações.
- Manter **reuniões semanais** de acompanhamento e cumprir o cronograma.
- Emitir **relatório mensal** com plano de ação e evidências; apoiar o aceite do contratante.

## 9. Obrigações da contratante

- Disponibilizar acesso às áreas, sistemas e informações necessários; designar fiscal/gestor; **avaliar e confrontar os relatórios mensais**, formalizando aceites/glosas, e aplicar penalidades quando cabível.

## 10. Indicadores de desempenho (mínimos)

- % de mapeamento concluído por secretaria (meta: ≥95% até o mês 4).
- % de políticas/POPs implantados (meta: ≥90% até o mês 8).
- Implantação e operação do **Canal do Titular** (meta: ativo até o mês 6).
- Capacitações realizadas (meta: 100% das previstas; presença mínima por turma).
- Evidências para **i-Gov TI/IEG-M** consolidadas (meta: 100% até o mês 11).

## 11. Prazos

- **Prazo total:** 12 meses, contados da OS de início.

## 12. Critérios de aceite

- Aceite mensal condicionado à entrega dos relatórios, evidências e marcos do cronograma; aceite final mediante: inventário consolidado, pacote completo de políticas/POPs, Canal do Titular ativo, trilha de capacitação concluída e dossiê de evidências i-Gov TI.

## 13. Reuniões e disponibilidade

- **Encontros semanais (1–2x/semana)**, preferencialmente presenciais, 2h, com atas e planos de ação registrados.

## 14. Sigilo e propriedade intelectual

- Todos os artefatos produzidos serão de propriedade da Prefeitura; a contratada deve **zelar pela confidencialidade e sigilo** das informações acessadas.

## 15. Condições comerciais (para cotação)

- **Preço global mensal** pelos serviços **incluindo todos os custos e despesas** (deslocamentos, alimentação e eventuais hospedagens). **Não** será admitida cobrança acessória por reuniões presenciais semanais ou por emissão de certificados, relatórios e evidências