MUNICÍPIO DE DIVISA NOVA
Rua Rio de Janeiro, nº 06 - Centro
37134-000 - Divisa Nova – Telefax: (35) 3286-1200
email: secretaria@divisanova.mg.gov.br

DECRETO Nº 2.187/2026, de 08 de julho de 2026

"DISPÕE SOBRE A APROVAÇÃO DO CÓDIGO DE CONDUTA DE PROTEÇÃO DE DADOS DA PREFEITURA DE DIVISA NOVA-MG E DÁ OUTRAS PROVIDÊNCIAS".

O Prefeito Municipal de Divisa Nova, no uso de suas atribuições,

DECRETA:

Artigo 1º - Fica aprovado o Código de Conduta de Proteção de Dados da Prefeitura Municipal, aprovado pelos membros do Comitê Municipal de Proteção de Dados Pessoas, cuja cópia faz parte integrante deste Decreto.

Artigo 2º - Este decreto entra em vigor na data de sua publicação.

Divisa Nova, em 08 de julho de 2026

JOSÉ LUIZ DE FIGUEIREDO
Prefeito Municipal

PUBLICADO
no mural do Paço Municipal de DIVISA NOVA-MG
Em: 08 / 07 / 2026
Servidor Responsável

Prefeitura Municipal de Divisa Nova/MG
Departamento de Tecnologia da Informação (TI).
Av. Padre Canton, 138 - Centro, Divisa Nova/MG.
Telefone: (35) 3286-1200 ramal: (249)
dpo@divisanova.mg.gov.br

CÓDIGO DE CONDUTA PARA PROTEÇÃO DE DADOS PESSOAIS

PREFEITURA MUNICIPAL DE DIVISA NOVA - MG

1. INTRODUÇÃO E OBJETIVO

Este Código de Conduta estabelece as diretrizes e normas de comportamento para todos os agentes públicos (servidores efetivos, comissionados, estagiários e prestadores de serviços) da Prefeitura Municipal de Divisa Nova, no que tange ao tratamento de dados pessoais, em estrita observância à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD).

O objetivo deste documento é assegurar que o tratamento de dados pessoais realizado pela Administração Pública Municipal ocorra de forma ética, segura e transparente, garantindo os direitos fundamentais de liberdade e de privacidade dos cidadãos.

2. PRINCÍPIOS FUNDAMENTAIS DA LGPD

Art. 6º da LGPD — Aplicação Prática no Município

Todas as atividades de tratamento de dados pessoais na Prefeitura devem observar a boa-fé e os seguintes princípios, aplicáveis a todas as categorias de titulares cujos dados são tratados pelo município: servidores e funcionários, cidadãos usuários de serviços públicos, contribuintes e fornecedores.

Princípio	Aplicação Prática no Município
Finalidade	Os dados coletados pela prefeitura abrangem diferentes categorias de titulares e devem ser utilizados **exclusivamente** para as finalidades que justificaram sua coleta, entre elas: **Servidores e Funcionários:** dados pessoais completos (nome, CPF, RG, endereço, filiação), dados bancários (pagamento de salário), dados de saúde (atestados, perícias, plano de saúde), dados previdenciários (INSS, RPPS), informações funcionais (cargo, lotação, histórico disciplinar) e **dados biométricos — incluindo a fotografia facial coletada no sistema de ponto eletrônico e os dados do crachá funcional**, classificados como dados pessoais sensíveis (Art. 5º, II da LGPD). A fotografia usada para reconhecimento facial no ponto é um **dado biométrico** e só pode ser utilizada para a finalidade exclusiva de controle de frequência, sendo vedado qualquer outro uso sem nova base legal. **Cidadãos/Usuários de Serviços:** Cadastro Único, Prontuário de Saúde, Matrícula Escolar, licenças e alvarás, cadastros de assistência social e benefícios. **Contribuintes:** dados fiscais e tributários (IPTU, ISS, taxas municipais, cadastros imobiliários e mobiliários). **Fornecedores e Contratados (PF):** CPF, dados bancários, certidões negativas e dados de habilitação em licitações. Cada conjunto de dados deve ser tratado apenas para a finalidade específica que o originou, não podendo ser reutilizado para propósitos incompatíveis sem nova base legal.
Adequação	O tratamento deve ser compatível com as finalidades informadas ao cidadão, ao servidor ou ao fornecedor no momento da coleta. Exemplos de inadequação que devem ser evitados:

Prefeitura Municipal de Divisa Nova/MG
Departamento de Tecnologia da Informação (TI).
Av. Padre Canton, 138 - Centro, Divisa Nova/MG.
Telefone: (35) 3286-1200 ramal: (249)
dpo@divisanova.mg.gov.br

	Dados de saúde (atestados, prontuários, perícias médicas de servidores) **não podem ser usados para fins de cobrança tributária** ou processos disciplinares, salvo base legal específica. **Dados do Cadastro Único** não podem ser utilizados para fins de cobrança de débitos municipais. **Fotografia facial e dados biométricos do ponto eletrônico:** coletados exclusivamente para controle de frequência, **não podem ser utilizados para monitoramento comportamental, investigações disciplinares, compartilhamento com outras secretarias ou fornecimento a terceiros** sem base legal específica. O uso da imagem facial para qualquer finalidade além do registro de ponto configura desvio de finalidade e violação da LGPD. **Dados do crachá funcional** (nome, foto, matrícula, setor): devem ser usados apenas para identificação funcional, não podendo ser reaproveitados para criação de bases de dados não autorizadas. Antes de compartilhar dados entre secretarias ou com outros órgãos, deve-se verificar se a nova finalidade é compatível com aquela original.
Necessidade	Deve-se coletar **apenas o mínimo de dados necessários** para atingir a finalidade. Antes de incluir um campo em qualquer formulário, sistema ou cadastro, deve-se questionar: "Este dado é realmente indispensável?" Exemplos práticos de aplicação do princípio da necessidade: **Formulários de serviços ao cidadão:** avaliar se é necessário solicitar CPF e RG simultaneamente, ou se apenas um documento já é suficiente para identificação. **Ficha de funcionários:** dados de saúde devem ser coletados apenas quando exigidos por lei (ex.: exame admissional, perícia) e mantidos separados dos demais dados funcionais. **Ponto eletrônico com foto e crachá:** avaliar se o sistema de reconhecimento facial é o único meio viável de controle de frequência ou se métodos menos invasivos (ex.: apenas crachá com QR Code) seriam suficientes. Quando o reconhecimento facial for adotado, a imagem deve ser convertida em template biométrico criptografado, **não sendo necessário armazenar a fotografia original** além do momento da captura. **Crachá funcional:** deve conter apenas as informações estritamente necessárias para identificação (nome, foto, setor), evitando dados adicionais desnecessários. **Sistemas de videomonitoramento:** imagens devem ser retidas apenas pelo período necessário e em áreas que justifiquem o monitoramento. **Cadastros tributários:** solicitar apenas os dados exigidos pela legislação fiscal vigente, sem campos adicionais desnecessários.
Livre Acesso	O cidadão, o servidor e qualquer titular têm o direito de consultar, de forma **facilitada e gratuita**, quais dados a prefeitura possui sobre eles e como estão sendo tratados. Para garantir esse direito: **Canal de atendimento:** disponibilizar formulário ou protocolo específico para solicitações de acesso a dados pessoais nos balcões de atendimento e no Portal do Cidadão. **Prazo de resposta:** atender às solicitações em prazo razoável, conforme regulamentação da ANPD. **Servidores e funcionários:** garantir acesso ao histórico funcional, dados de folha de pagamento e informações de saúde ocupacional que constem nos sistemas da prefeitura. **Sistemas internos:** registrar e documentar quais dados são tratados em cada sistema, facilitando o atendimento de solicitações de acesso.
Qualidade dos Dados	A prefeitura deve garantir que os dados sejam **exatos, claros, relevantes e atualizados**, especialmente antes de tomar decisões que afetem o cidadão ou o servidor. Medidas práticas: **Benefícios sociais:** verificar e atualizar os dados do Cadastro Único periodicamente,

	evitando concessão ou cancelamento indevido de benefícios com base em informações desatualizadas. **Folha de pagamento:** manter dados bancários, endereços e dependentes dos servidores atualizados para evitar erros em pagamentos e benefícios. **Cadastros tributários:** garantir a atualização de dados de proprietários de imóveis e empresas para evitar lançamentos incorretos de IPTU e ISS. **Prontuários de saúde:** assegurar que históricos médicos e medicamentos estejam corretos antes de decisões clínicas. **Procedimento:** instituir rotina periódica de revisão e atualização dos principais cadastros, com responsáveis definidos em cada secretaria.
Transparência	Devem ser fornecidas **informações claras e acessíveis** sobre o tratamento de dados pessoais realizados pela prefeitura. Formas de garantir a transparência: **Portal da Transparência:** publicar o Registro de Atividades de Tratamento (RAT), identificando quais dados são tratados, com qual finalidade, base legal e por quanto tempo são retidos. **Balcões de atendimento:** disponibilizar material informativo sobre como os dados coletados serão utilizados. **Termos de coleta:** incluir avisos de privacidade (informações sobre finalidade, base legal e direitos do titular) em formulários físicos e digitais. **Servidores — ponto eletrônico com foto e crachá:** os servidores devem ser **formalmente informados**, de forma clara e prévia, que: (a) sua fotografia facial é coletada como dado biométrico sensível; (b) a finalidade é exclusivamente o controle de frequência; (c) quem tem acesso a esses dados; (d) por quanto tempo são retidos; e (e) quais são seus direitos como titular. Essa comunicação deve ser feita por escrito, preferencialmente na admissão e sempre que houver mudança no sistema. **Servidores — monitoramento geral:** informar claramente quais dados funcionais são monitorados (uso de sistemas, controle de acesso, ponto eletrônico) e com qual finalidade. **Contratações:** incluir cláusulas de proteção de dados nos contratos com fornecedores que tratem dados pessoais da prefeitura, especialmente os fornecedores do sistema de ponto eletrônico.
Segurança	Utilização de **medidas técnicas e administrativas** para proteger os dados de acessos não autorizados, perdas, alterações ou comunicações indevidas. Medidas essenciais: **Controle de acesso:** cada servidor deve ter login individual com senha, acessando apenas os sistemas e informações necessários ao exercício de suas funções (princípio do menor privilégio). **Proteção de sistemas:** uso de antivírus, firewall, criptografia de dados sensíveis e autenticação em dois fatores para sistemas críticos. **Dados biométricos do ponto eletrônico (foto facial e crachá):** por serem dados **sensíveis**, exigem proteção reforçada: (a) armazenamento criptografado dos templates biométricos; (b) acesso restrito apenas ao setor de RH e ao gestor do sistema; (c) proibição de exportação ou cópia das imagens faciais; (d) o fornecedor do sistema deve assinar contrato como **operador de dados**, com cláusulas específicas de segurança e sigilo; (e) registros (logs) de todos os acessos ao sistema de ponto devem ser mantidos e auditáveis. **Crachás perdidos ou roubados:** deve existir procedimento formal de comunicação e bloqueio imediato do crachá, com registro do ocorrido. **Dados de servidores:** fichas funcionais, dados de saúde e folha de pagamento devem ter acesso restrito ao RH e setores autorizados. **Contratos e licitações:** documentos com dados de fornecedores e contratados devem ser protegidos contra acesso não autorizado. **Descarte seguro:** documentos físicos com dados pessoais devem ser destruídos por meio de fragmentação (trituração); arquivos digitais devem ser deletados de forma

	segura. **Treinamento:** capacitar servidores sobre procedimentos de segurança da informação.
Prevenção	Adoção de **medidas proativas** para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Exemplos de medidas preventivas: **Bloqueio automático de telas:** configurar todos os computadores para bloquear a tela após período de inatividade, evitando acesso indevido a sistemas com dados pessoais. **Senhas individuais e intransferíveis:** proibir o compartilhamento de senhas de acesso aos sistemas municipais. **Ponto eletrônico com foto facial:** antes de implantar ou renovar contrato de sistema de ponto com reconhecimento facial, elaborar **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**, por se tratar de tratamento de dados biométricos em larga escala — o que configura tratamento de alto risco nos termos da LGPD. O RIPD deve avaliar os riscos e as medidas de mitigação adotadas. **Crachás funcionais:** estabelecer política formal de emissão, uso, controle e bloqueio de crachás, incluindo procedimento de comunicação obrigatória em caso de perda ou furto. **Treinamentos periódicos:** capacitar servidores para reconhecer tentativas de phishing, engenharia social e outros riscos cibernéticos. **Avaliação antes de novos sistemas:** realizar RIPD antes de implantar novos sistemas que envolvam tratamento de dados sensíveis. **Política de mesa limpa:** documentos físicos com dados pessoais não devem ficar expostos em mesas ou impressoras. **Backups regulares:** realizar cópias de segurança dos dados para evitar perda por falha técnica ou ataques.
Não Discriminação	É **proibido** o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos. Aplicações práticas no contexto municipal: **Seleção de pessoal:** dados de saúde, religião, orientação sexual, origem étnica ou convicções políticas de candidatos a cargos públicos não podem ser utilizados como critério de seleção ou eliminação. **Concessão de benefícios:** o acesso a serviços públicos e benefícios sociais não pode ser negado com base em dados que gerem discriminação indevida. **Servidores:** informações sobre doenças, gravidez, condição socioeconômica ou crença religiosa dos servidores não podem influenciar promoções, remoções ou processos disciplinares. **Cadastros tributários:** a cobrança de tributos deve ser baseada em critérios objetivos e legais, sem uso discriminatório de dados pessoais. **Fiscalização:** o exercício do poder de polícia administrativa (vigilância sanitária, fiscal, etc.) não pode ser direcionado com base em dados discriminatórios dos titulares.
Responsabilização	A prefeitura deve ser capaz de **demonstrar que adotou medidas eficazes** para o cumprimento das normas de proteção de dados pessoais. Para isso, recomenda-se: **Designar o Encarregado (DPO):** nomear formalmente o responsável pela proteção de dados pessoais e divulgar seu contato publicamente. **Registro de Atividades de Tratamento (RAT):** documentar todas as operações de tratamento realizadas pelas secretarias (finalidade, base legal, dados tratados, prazo de retenção), incluindo obrigatoriamente o tratamento de **dados biométricos do ponto eletrônico (foto facial e crachá)**, com identificação do sistema utilizado, do fornecedor e das medidas de segurança adotadas. **Políticas internas:** elaborar e implementar Política de Privacidade e Proteção de Dados, Política de Segurança da Informação e normas de uso dos sistemas. **Relatório de Impacto (RIPD):** elaborar obrigatoriamente para o sistema de ponto eletrônico com reconhecimento facial, por envolver tratamento de dados biométricos

em larga escala. Também obrigatório para demais tratamentos de alto risco envolvendo dados sensíveis de servidores, cidadãos vulneráveis ou crianças.

Contratos com fornecedores: o contrato com a empresa fornecedora do sistema de ponto eletrônico deve conter **cláusulas de operador de dados**, definindo responsabilidades, proibição de uso indevido das imagens, medidas de segurança exigidas e obrigações em caso de incidente.

Treinamentos: registrar e documentar as capacitações realizadas com servidores sobre a LGPD.

Gestão de incidentes: ter procedimento formal para identificar, comunicar e responder a incidentes de segurança envolvendo dados pessoais, incluindo vazamento de dados biométricos.

Contratos gerais: incluir cláusulas de proteção de dados em todos os contratos com fornecedores e parceiros que tratem dados pessoais em nome da prefeitura.

3. DEVERES DOS AGENTES PÚBLICOS

No exercício de suas funções, todos os colaboradores da Prefeitura devem:

1. Sigilo Profissional: Manter sigilo sobre todos os dados pessoais a que tiverem acesso em razão do cargo ou função, mesmo após o término do vínculo com a municipalidade.

2. Acesso Restrito: Acessar apenas os sistemas e dados estritamente necessários para a realização de suas tarefas diárias.

3. Segurança Digital: Não compartilhar senhas de acesso, não deixar computadores logados sem supervisão e utilizar apenas dispositivos oficiais para o tratamento de dados.

4. Descarte Seguro: Garantir que documentos físicos contendo dados pessoais sejam descartados de forma a impossibilitar a leitura (fragmentação), e não apenas jogados no lixo comum.

5. Comunicação de Incidentes: Informar imediatamente ao Encarregado de Dados (DPO) qualquer suspeita de vazamento, perda ou acesso indevido a dados pessoais, incluindo perda ou roubo de crachá funcional e qualquer falha no sistema de ponto eletrônico com reconhecimento facial.

6. Dados Biométricos e Crachá Funcional: Zelar pelo uso adequado do crachá funcional e do sistema de ponto eletrônico com reconhecimento facial, sendo expressamente proibido: (a) emprestar ou ceder o crachá a terceiros; (b) tentar burlar ou fraudar o sistema de reconhecimento facial; (c) fotografar, copiar ou reproduzir dados exibidos no crachá de outros servidores; (d) utilizar o crachá ou os dados do ponto eletrônico para fins diversos do controle de frequência. Em caso de perda, furto ou dano ao crachá, o servidor deve comunicar imediatamente ao setor de RH para bloqueio e emissão de nova via.

7. Acesso Remoto e Dispositivos Pessoais: O acesso a sistemas municipais que contenham dados pessoais deve ser realizado exclusivamente por meio de dispositivos e redes oficiais ou autorizadas pela prefeitura. O uso de dispositivos pessoais (celulares, tablets, notebooks particulares) para tratamento de dados pessoais de titulares somente é permitido mediante autorização formal do setor de TI e com adoção das medidas de segurança estabelecidas pela prefeitura.

4. O ENCARREGADO PELO TRATAMENTO DE DADOS (DPO)

A Prefeitura Municipal de Divisa Nova designou formalmente o Encarregado pelo Tratamento de Dados Pessoais (DPO), conforme exigido pelo Art. 41 da LGPD. O contato do Encarregado é público e pode ser acessado por qualquer titular de dados: **dpo@divisanova.mg.gov.br**. Solicitações, dúvidas e comunicações sobre proteção de dados devem ser encaminhadas a esse canal e pelo telefone (35)3286-1200 ramal: 249.

São atribuições do Encarregado (Art. 41, §2º da LGPD):

1. Aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências;

2. Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar as providências necessárias;

3. Orientar os servidores e os contratados da prefeitura a respeito das práticas a serem adotadas em relação à proteção de dados pessoais;

4. Elaborar, manter e atualizar o Registro de Atividades de Tratamento (RAT), documentando todas as operações de tratamento de dados pessoais realizadas pela prefeitura, incluindo o tratamento de dados biométricos do sistema de ponto eletrônico;

5. Promover e coordenar treinamentos e capacitações periódicas sobre a LGPD junto às secretarias e setores da prefeitura, mantendo registro das ações realizadas;

6. Coordenar e elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando o tratamento envolver dados sensíveis ou representar alto risco aos titulares, especialmente no caso do sistema de ponto eletrônico com reconhecimento facial;

7. Coordenar a resposta a incidentes de segurança envolvendo dados pessoais, comunicando a ANPD e os titulares afetados nos prazos legais, quando necessário.

5. RELACIONAMENTO COM TERCEIROS E FORNECEDORES

Todos os contratos administrativos e convênios celebrados pela Prefeitura que envolvam o compartilhamento ou tratamento de dados pessoais devem conter cláusulas específicas de conformidade com a LGPD, exigindo dos terceiros o mesmo nível de proteção adotado pelo Município.

Quando um fornecedor tratar dados pessoais em nome da Prefeitura, ele assume a condição de **operador de dados** (Art. 39 da LGPD). É o caso, por exemplo, da empresa fornecedora do sistema de ponto eletrônico com reconhecimento facial, que processa dados biométricos dos servidores. Os contratos com operadores de dados devem obrigatoriamente prever:

1. Tratamento dos dados apenas conforme as instruções da Prefeitura e para as finalidades contratadas, sendo vedado uso para fins próprios ou de terceiros;

2. Adoção de medidas técnicas e administrativas de segurança adequadas ao nível de risco do tratamento, especialmente para dados biométricos e sensíveis;

3. Proibição de subcontratação do tratamento de dados sem autorização prévia e expressa da Prefeitura;

4. Notificação imediata à Prefeitura, em até 24 horas, em caso de qualquer incidente de segurança que envolva dados pessoais tratados em nome do Município;

5. Devolução ou exclusão segura de todos os dados pessoais ao término do contrato, com comprovação formal;

6. Responsabilidade solidária do operador pelos danos causados em razão de tratamento realizado em descumprimento das instruções legítimas da Prefeitura ou da LGPD.

6. DISPOSIÇÕES FINAIS E SANÇÕES

O descumprimento das diretrizes deste Código de Conduta sujeitará o infrator às sanções administrativas previstas no Estatuto dos Servidores Públicos Municipais, sem prejuízo de eventuais responsabilidades civis e criminais.

Adicionalmente, na condição de controladora de dados, a Prefeitura Municipal de Divisa Nova está sujeita às sanções administrativas previstas no Art. 52 da LGPD, aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD), que incluem: advertência com prazo para adoção de medidas corretivas; publicização da infração; bloqueio ou eliminação dos dados pessoais; e suspensão parcial ou total do banco de dados. A prevenção dessas sanções reforça a responsabilidade de todos os agentes públicos no cumprimento deste Código.

Este Código entra em vigor na data de sua publicação e deve ser amplamente divulgado em todas as secretarias municipais, sendo obrigatória sua leitura e ciência por todos os servidores, estagiários e prestadores de serviços no ato da admissão ou renovação de contrato.

Este Código será revisado anualmente ou sempre que ocorrer alteração normativa relevante na legislação de proteção de dados, ficando o Encarregado (DPO) responsável por propor as atualizações necessárias junto ao Comitê Municipal de Proteção de Dados Pessoais (CMPDP), que as submeterá ao Chefe do Executivo Municipal.

Divisa Nova – MG, 08 de julho de 2026

Eduardo José da Silva
Encarregado de Proteção de Dados Pessoais e Cibersegurança
Presidente do Comitê Municipal de Proteção de Dados Pessoais