Resolução nº 316, de 15 de dezembro de 2025

Institui a política geral de privacidade e proteção de dados pessoais no âmbito do poder legislativo de Jaru/RO.

A MESA DIRETORA DA CÂMARA MUNICIPAL DE JARU/RO, no uso de suas atribuições legais, faz saber que o PLENÁRIO aprovou e ela promulga a seguinte resolução:

Considerando a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que estabelece regras para a coleta, tratamento, armazenamento e compartilhamento de dados pessoais, tanto em meios físicos quanto digitais, por pessoas físicas ou jurídicas.

Considerando a Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso 11 do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

Considerando o disposto no art. 6º, III, c/c art. 4º, IV da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), que trata da proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso;

Considerando a necessidade de preservar o dever de transparência, sedimentado na Lei de Responsabilidade Fiscal e na Lei de Acesso à Informação (LAI), e o dever de proteção de dados pessoais, de que trata a Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando o Ato nº 5/2023/MD/CMJ que regulamenta a aplicação da Lei n. 13.709, de 14 de agosto de 2018. - Lei Geral de Proteção de Dados Pessoais (LGPD), no âmbito da Câmara Municipal de Jaru.

Considerando que o tratamento de dados pessoais pode envolver múltiplas unidades administrativas e fornecedores, bem como diferentes meios e tecnologias de coleta, processamento, armazenamento e comunicação de informações;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Instituir no âmbito do Poder Legislativo de Jaru, a Política Geral de Privacidade e Proteção de Dados Pessoais, aplicável aos meios físicos e digitais, como parte integrante de sua estrutura normativa, observando os princípios, diretrizes e objetivos compatíveis com os requisitos estabelecidos na legislação brasileira vigente.

§1º Esta Política estabelece diretrizes para a proteção de dados pessoais no âmbito do Poder Legislativo, que atua como controlador no tratamento de dados. Aplica-se também a qualquer pessoa, interna ou externa, que realize operações de tratamento de dados pessoais em nome do Poder Legislativo ou em suas dependências.

§2º Esta política, não se aplica ao tratamento de dados pessoais realizados por gabinetes parlamentares, lideranças partidárias, frentes parlamentares e Comissões Temáticas, quando o tratamento não utilizar sistemas institucionais da Câmara Municipal de Jaru.

CAPÍTULO II
GLOSSÁRIO

Art. 2º Para os efeitos desta Resolução, seguem as definições a seguir:

I - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

II - Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, em todas as instâncias da instituição ou no âmbito de contratos ou instrumentos congêneres firmados com ele;

III - Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre este, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

IV - Encarregado substituto: pessoa indicada pelo controlador para substituir o encarregado titular;

V - Dado pessoal: informação relacionada à pessoa natural identificada ou identificável, ou seja, qualquer informação que permita identificar, direta ou indiretamente, um indivíduo;

VI - 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;

VII - Dado anonimizado: dado relativo a um indivíduo que não possa ser identificado, pois passou por algum meio técnico de tratamento para garantir sua desvinculação, direta ou indireta, a uma pessoa;

VIII - Banco de dados: conjunto estruturado de dados pessoais, estabelecido em meio físico ou eletrônico;

IX - Titular de dados: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

X - Tratamento de dados pessoais: toda operação exercida sobre dados pessoais, compreendendo a coleta, a produção, a recepção, a classificação, a utilização, o acesso, a reprodução, a transmissão, a distribuição, o processamento, o arquivamento, o armazenamento, a eliminação, a avaliação ou o controle da informação, a modificação, a comunicação, a transferência, a difusão ou a extração;

XI - Agentes de tratamento: o controlador e o operador;

XII - Anonimização: utilização de meios técnicos razoáveis que impossibilitem que um dado seja associado, direta ou indiretamente, a um indivíduo;

XIII - Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIV - Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XV - Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XVI - Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVII - Compartilhamento de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais entre órgãos públicos e privados nos cumprimentos de suas competências legais;

XVIII - Relatório de impacto na proteção de dados pessoais: documentação do controlador com a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como das medidas e mecanismos de mitigação de risco; e

XIX - Autoridade Nacional de Proteção de Dados ANPD: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da legislação de proteção de dados pessoais em todo o território nacional.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Art. 3º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - Legítima, específica e explícita, que deverá ser informada ao titular, sendo vedado o tratamento posterior dos dados para outras finalidades e fins discriminatórios, ilícitos ou abusivos;

II - Adequação do tratamento dos dados pessoais, compatível com as finalidades informadas ao titular;

III - Necessidade do tratamento dos dados pessoais limitada aos objetivos para os quais serão processados, abrangendo somente os dados pertinentes, proporcionais e não excessivos, em relação à finalidade do tratamento de dados para a qual foram coletados;

IV - Garantia, ao titular, de livre acesso, de forma gratuita e facilitada, ao tratamento de seus dados pessoais;

V - Garantia, ao titular, de exatidão, clareza, relevância e atualização de seus dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Garantia, ao titular, de acesso facilitado a informações claras e precisas sobre a realização do tratamento de seus dados pessoais e os respectivos agentes de tratamento;

VII - Utilização de medidas técnicas e administrativas de segurança e prevenção adequadas ao tratamento e à proteção de dados pessoais nos casos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Proibição do tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos; e

IX - Responsabilização e prestação de contas dos agentes de tratamento quanto ao dever de cumprir as normas legais e regulatórias de proteção de dados pessoais.

Art. 4º O objetivo geral desta Resolução é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à proteção de dados pessoais e dos direitos de seus titulares no âmbito do Poder Legislativo de Jaru.

Parágrafo único. São objetivos específicos desta Resolução:

I - Assegurar níveis adequados de proteção aos dados pessoais tratados pelo Poder Legislativo de Jaru;

II - Orientar quanto à adoção de controles técnicos e administrativos para atendimento dos requisitos de proteção de dados pessoais;

III - Garantir aos titulares de dados pessoais os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural;

IV - Prevenir possíveis causas de violações de dados pessoais e incidentes de segurança da informação relacionados ao tratamento de dados pessoais; e

V - Minimizar os riscos de violação de dados pessoais tratados pelo Poder Legislativo de Jaru e qualquer impacto negativo decorrente dessa violação.

CAPÍTULO IV
DOS ATORES E DAS RESPONSABILIDADES

Art. 5º No Poder Legislativo de Jaru, o Controlador é a Câmara Municipal de Jaru representada pelo (a) Presidente, que exercerá suas atribuições com auxílio do Comitê Gestor de proteção de dados-CGPD, instituído no âmbito da Câmara Municipal, respeitadas suas respectivas competências e campos funcionais e deverá:

I - Observar os fundamentos, princípios da privacidade e proteção de dados pessoais, bem como os deveres impostos pela LGPD e por normativos correlatos, no momento de decidir sobre um futuro tratamento ou realizá-lo;

II - Considerar o disposto nos artigos 7º, 11 e 23 da LGPD antes de realizar o tratamento de dados pessoais;

III - Cumprir o previsto nos artigos 46 e 50 da LGPD, visando à proteção dos dados pessoais e à promoção da sua governança;

IV - Indicar um encarregado pelo tratamento de dados pessoais, divulgando sua identidade e informações de contato de forma clara e objetiva no sítio institucional;

V - Indicar um encarregado substituto, para exercer as funções conforme a necessidade e em caso de impedimento ou impossibilidade do encarregado titular;

VI - Realizar o mapeamento de dados pessoais, inclusive os dados sensíveis, identificando e categorizando toda e qualquer relação de coleta, armazenamento e tratamento de dados pessoais;

VII - Reter os dados pessoais apenas pelo período necessário ao cumprimento da hipótese legal e da finalidade que fundamenta o tratamento;

VIII - Criar e manter atualizados os avisos ou políticas de privacidade, informando sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, bem como as formas de proteção aplicadas;

IX - Elaborar relatório de impacto à proteção de dados pessoais (RIPD), inclusive em relação aos dados sensíveis, com base no mapeamento de dados realizado pelas unidades administrativas do Poder Legislativo;

X - Avaliar e apresentar, por meio de relatório, o nível de risco relacionado aos departamentos responsáveis pelo tratamento de dados pessoais, abrangendo as atividades de coleta, uso, reprodução, transmissão, armazenamento, eliminação e arquivamento;

XI - Orientar os operadores quanto ao tratamento de dados pessoais, conforme as instruções internas, a legislação vigente e as regulamentações da ANPD;

XII - Promover a conscientização contínua sobre a importância da proteção de dados pessoais no âmbito do órgão ou entidade.

Art. 6º Compete ao operador:

I - Observar os princípios estabelecidos no art. 6º da Lei Geral de Proteção de Dados Pessoais (LGPD), ao realizar qualquer tratamento de dados pessoais;

II - Seguir as diretrizes estabelecidas pelo controlador, em conformidade com o disposto nos artigos 7º, 11 e 22 da LGPD;

III - Tratar os dados pessoais conforme as instruções formalmente repassadas pelo controlador, zelando pela correta execução dessas diretrizes, mantendo registros das operações realizadas, garantindo a segurança e a confidencialidade das informações, e sujeitando-se às sanções legais em caso de descumprimento.

Parágrafo único. É vedada ao operador a tomada de decisão unilateral quanto aos meios e às finalidades utilizados no tratamento de dados pessoais.

Art. 7º O encarregado é responsável por:

I - Receber as reclamações e comunicações dos titulares;

II - Encaminhar internamente a demanda para as unidades competentes;

III - Receber as comunicações da ANPD e adotar as providências necessárias;

IV - Orientar todos os colaboradores do Poder Legislativo de Jaru sobre as práticas a serem adotadas em relação à proteção de dados pessoais; e

V - Executar outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares da ANPD.

Art.8º São atribuições do Comitê Gestor de Proteção de Dados Pessoais - CGPDP:

I - Fornecer as instruções para a política de tratamento de dados pessoais e respectivos programas, incluindo a forma como os dados serão tratados no âmbito do Poder Legislativo do Município de Jaru/RO, a aplicação da metodologia de gestão de riscos no tratamento de dados e a segurança da informação;

II - Estabelecer que o tratamento de dados ocorra com ética, critério e responsabilidade;

III - Comunicar à autoridade superior e ao titular dos dados, em prazo razoável, a ocorrência de incidentes de segurança com dados pessoais que possam causar danos ou representar risco relevante ao titular;

IV - Propor ao Presidente desta Casa de Leis a edição de regras e políticas de privacidade de dados pessoais;

V - Proteger a privacidade dos dados pessoais, tanto de usuários quanto de servidores do Poder Legislativo;

VI - Assessorar o controlador e os operadores da LGPD no âmbito deste Poder Legislativo;

VII - Promover a conscientização dos servidores, elaborar cartilhas, manuais de boas práticas relacionadas ao tratamento de dados pessoais; e

VIII - Realizar demais atividades correlatas.

Art. 9º Os servidores e demais colaboradores vinculados ao Poder Legislativo de Jaru são responsáveis por:

I - Realizar atividades de tratamento de dados pessoais, sob a coordenação e orientação do controlador;

II - Ler e cumprir integralmente os termos desta Resolução, bem como as demais normas e procedimentos de proteção da privacidade e de dados pessoais aplicáveis;

III - Comunicar ao encarregado qualquer evento que viole esta Resolução ou coloque em risco os dados pessoais tratados pelo Poder Legislativo de Jaru; e

IV - Responder, no âmbito do Poder Legislativo de Jaru, pela inobservância da política instituída nesta Resolução e das demais normas e procedimentos legais ou regulatórios relacionados ao tratamento de dados pessoais.

CAPÍTULO V
DO TRATAMENTO DE DADOS PESSOAIS

Art. 10 O tratamento de dados pessoais compreende todas as operações realizadas desde a coleta inicial até o descarte final das informações, incluindo o armazenamento e a utilização. Esse tratamento, seja de forma conjunta ou isolada, somente poderá ocorrer nas seguintes hipóteses:

I - Mediante o consentimento do titular;

II - Para o cumprimento de obrigação legal ou regulatória;

III - Para a execução de políticas públicas, incluindo o tratamento e uso compartilhado de dados;

IV- Para a realização de estudos por órgão de pesquisa, assegurada a anonimização dos dados pessoais sempre que possível;

V - Para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular;

VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

VII - Para a proteção da vida ou da segurança física do titular ou de terceiro;

VIII - Para a tutela da saúde em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - Quando necessário para atender a legítimo interesse do controlador ou de terceiro;

X - Para a proteção de crédito, inclusive quanto ao disposto na legislação pertinente; e

XI - Para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as suas competências ou cumprir suas atribuições legais.

§1º. O consentimento para a coleta de dados pessoais deverá ser obtido de forma livre, expressa, individual, clara, específica e legítima e poderá ser revogado a qualquer momento pelo titular, conforme modelo em anexo I desta resolução.

§2º. O consentimento é dispensado para o tratamento de dados pessoais tornados manifestamente públicos pelo titular, desde que o tratamento seja realizado de acordo com a finalidade, a boa-fé e o interesse público, resguardados os direitos do titular.

Art. 11 O tratamento de dados sensíveis será realizado com o consentimento do titular ou de seu responsável legal de forma específica e destinado a finalidades específicas.

§1º. O consentimento de que trata o caput deste artigo será dispensado:

I - Nas hipóteses previstas nos incisos II ao XI do artigo 10 desta Resolução;

II - Nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, para prevenir fraudes e garantir a segurança dos dados pessoais do titular, resguardados todos os direitos de privacidade e proteção desses dados.

§2º. Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

Art. 12 Os dados anonimizados não serão considerados dados pessoais para os fins das diretrizes previstas nesta Resolução, salvo quando for revertido o processo de anonimização ao qual foram submetidos.

Parágrafo único. Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Art. 13 O tratamento de dados pessoais de crianças e de adolescentes tem a finalidade de atender a seu melhor interesse e deverá ser realizado com o consentimento expresso e em destaque de um dos pais ou responsável legal, bem como ser específico quanto à finalidade do tratamento.

Parágrafo único. A informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos de tratamento dos dados pessoais de que trata o caput deste artigo deverá ser mantida pública.

Art. 14 Os dados pessoais divulgados por este Poder Legislativo Municipal em sítios e portais eletrônicos, publicações em diário oficial eletrônico e demais publicações, em observância aos princípios da finalidade, necessidade, adequação, segurança, prestação de contas e prevenção, constantes da Lei Geral de Proteção de Dados Pessoais (LGPD), devem ficar anonimizados quando se revelarem desnecessários e não contrariarem o dever maior de publicidade e transparência, conforme detalhamento contido no anexo III desta Resolução.

Art. 15 O tratamento de dados pessoais deverá ser finalizado quando:

I - Quando for alcançada a finalidade para a qual os dados foram coletados ou quando esses dados deixarem de ser necessários ou pertinentes para essa finalidade;

II - Quando o período de tratamento chegar ao fim;

III - Quando houver pedido de revogação do consentimento feito pelo titular, resguardado o interesse público; ou

IV - Por determinação da ANPD, em caso de violação à Lei nº 13.709, de 14 de agosto de 2018.

Art. 16 Os dados pessoais serão eliminados após o término de seu tratamento, exceto nas seguintes hipóteses:

I - Cumprimento de obrigação legal ou regulatória;

II - Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - Transferência a terceiro, desde que respeitados os requisitos legais de tratamento de dados pessoais; ou

IV - Uso exclusivo pelo Poder Legislativo de Jaru, vedado seu acesso por terceiro e desde que anonimizados os dados.

Art. 17 O uso compartilhado de dados pelo Poder Legislativo de Jaru deverá ocorrer no cumprimento de suas obrigações legais ou regulatórias, com organizações públicas ou privadas, de acordo com a finalidade admitida na legislação pertinente, resguardados os princípios de proteção de dados pessoais.

Parágrafo único. Na prestação dos serviços de sua competência, o Poder Legislativo de Jaru compartilhará dados pessoais de acordo com a interoperabilidade de seus sistemas e serviços de tecnologia da informação, observada a norma administrativa pertinente.

Art. 18 São atividades que deverão ser realizadas no tratamento de dados pessoais:

I - Garantir ao titular a opção de permitir ou não o tratamento de seus dados pessoais, excetuando-se os casos de tratamento sem a necessidade de seu consentimento;

II - Assegurar que o objetivo do tratamento de dados pessoais esteja em conformidade com esta Resolução e com a legislação vigente;

III - Comunicar de forma clara o tratamento de dados pessoais ao titular antes do momento em que forem coletados ou usados pela primeira vez para nova finalidade;

IV - Quando requisitadas, fornecer ao titular explicações sobre o tratamento de seus dados pessoais;

V - Limitar a coleta, o uso, a divulgação e a transferência de dados pessoais ao necessário para o cumprimento da finalidade consentida pelo titular ou da base legal específica para o tratamento sem o consentimento;

VI - Reter dados pessoais apenas pelo tempo necessário para cumprir sua finalidade e, posteriormente, destruí-los, bloqueá-los ou anonimizá-los com segurança;

VII - Bloquear o acesso a dados pessoais quando, expirado o período de seu tratamento e sua manutenção, for exigido pela legislação;

VIII - Fornecer informações claras sobre as políticas, procedimentos e práticas de tratamento de dados pessoais a seus titulares;

IX - Cientificar os titulares quando ocorrerem alterações significativas no tratamento de seus dados pessoais;

X - Garantir aos titulares o acesso e a revisão de seus dados pessoais por meio de técnica adequada de autenticação de identidade, desde que não haja restrição legal ao acesso ou à revisão;

XI - Assegurar a rastreabilidade e a prestação de contas durante todo o tratamento de dados pessoais, inclusive daqueles compartilhados com terceiros;

XII - Gerenciar eventual violação aos dados tratados, mantendo o registro de incidentes e das respostas efetuadas;

XIII - Adotar controles técnicos e administrativos de segurança da informação suficientes para garantir níveis de proteção adequados; e

XIV - Assegurar que a elaboração e a publicação das decisões do Poder Legislativo de Jaru estejam em conformidade com a Lei nº 13.709, de 14 de agosto de 2018, no que se refere à minimização da utilização de dados pessoais.

Art. 19 No caso de transferência internacional de dados pessoais deverá ser observado o que consta no Capítulo V da LGPD.

CAPÍTULO VI
DIREITOS DOS TITULARES

Art. 20 Os titulares de dados pessoais têm o direito garantido, de acordo com a legislação vigente, de efetivar seus direitos, especialmente estabelecidos no artigo 18 da Lei Geral de Proteção de Dados - LGPD, e todas as formalidades relacionadas ao atendimento dessas solicitações. Nesse sentido, é facultado aos titulares de dados pessoais:

I - Confirmar a existência de tratamento de dados pessoais e obter, a qualquer tempo, acesso aos dados tratados;

II - Solicitar a correção de dados incompletos, inexatos ou desatualizados;

III - Requerer a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;

IV - Solicitar, de forma expressa, a portabilidade dos seus dados, quando pertinente;

V - Requisitar informações sobre as entidades públicas e privadas com as quais os dados foram compartilhados;

VI - Obter acesso às informações de identificação do controlador de dados e o contato do responsável;

VII - Requerer informações sobre a possibilidade da não concessão do consentimento para os tratamentos que o exigirem, bem como sobre as consequências da negativa; e, quando aplicável, revogar o consentimento e solicitar a exclusão dos dados tratados, preservados os prazos mínimos de guarda e manutenção de dados, nos termos da legislação.

§1º O titular terá acesso às informações sobre a coleta, o tratamento, o armazenamento, o compartilhamento e demais procedimentos relacionados aos seus dados, no prazo de até 15 (quinze) dias, contado do recebimento do requerimento.

§ 2º O titular poderá obter informações sobre o tratamento de seus dados e exercer os direitos previstos neste artigo a qualquer tempo, de forma facilitada pelo e-mail da ouvidoria@jaru.ro.leg.br ou por meio do canal de atendimento Fala.BR - Plataforma Integrada de Ouvidoria e Acesso à Informação, disponível no sítio deste Poder Legislativo, canal de atendimento da Ouvidoria da Câmara Municipal de Jaru.

CAPÍTULO VII
SEGURANÇA E BOAS PRÁTICAS

Art. 21 Serão adotadas medidas técnicas de Segurança da Informação que visam garantir a segurança e privacidade dos dados pessoais, prevenindo acessos não autorizados e vazamentos. Essas medidas abrangem:

I - Implementar a criptografia de dados pessoais e sensíveis, a fim de assegurar a confidencialidade das informações e prevenir acessos não autorizados;

II - Utilizar firewalls como barreiras de proteção para impedir acessos externos indevidos às redes, servidores e sistemas da Câmara Municipal;

III - Estabelecer mecanismos de controle de acesso lógico, por meio de autenticação e autorização, restringindo o acesso a dados pessoais apenas a usuários expressamente autorizados, conforme critérios de necessidade e função;

IV - Adotar sistemas de monitoramento contínuo da rede e dispositivos tecnológicos, com o objetivo de identificar e responder a atividades suspeitas ou tentativas de violação;

V - Implementar procedimentos de backup periódico e um plano de recuperação de desastres, garantindo a integridade, disponibilidade e continuidade dos dados;

VI - Instalar e manter atualizados softwares de proteção contra códigos maliciosos, como antivírus e anti-malware;

VII - Manter sistemas operacionais, aplicativos e plataformas tecnológicas atualizados, com a aplicação regular de correções e atualizações de segurança recomendadas pelos fabricantes;

VIII - Adotar, sempre que possível, técnicas de anonimização ou pseudonimização de dados pessoais, visando à mitigação de riscos relacionados à identificação dos titulares.

Art. 22 Serão adotadas medidas organizacionais de Segurança da Informação que visam garantir a segurança e o tratamento adequado dos dados pessoais, abrangendo desde a criação de políticas e procedimentos até a conscientização e capacitação dos colaboradores, sendo que essas medidas complementam as medidas técnicas e buscam evitar acessos não autorizados, divulgação indevida e outros incidentes relacionados aos dados.

I - Estabelecer, documentar e manter atualizadas as políticas internas, normas e procedimentos relacionados à proteção de dados pessoais e à segurança da informação;

II - Promover capacitações e ações de conscientização regulares voltadas aos servidores e colaboradores, abordando os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), boas práticas de segurança da informação e prevenção de incidentes;

III - Implantar processos contínuos de gestão de riscos, visando à identificação, avaliação e mitigação de riscos relacionados ao tratamento de dados pessoais;

IV - Garantir que o acesso a ambientes físicos onde haja tratamento de dados pessoais ocorra exclusivamente por pessoas previamente autorizadas;

V - Estabelecer e manter atualizado um plano de resposta a incidentes de segurança, com procedimentos para identificação, comunicação, contenção e mitigação de falhas envolvendo dados pessoais;

VI - Realizar auditorias internas periódicas para verificar a conformidade das medidas de proteção adotadas com os requisitos legais e regulatórios;

VII - Incluir cláusulas específicas de proteção de dados pessoais em contratos firmados com fornecedores, prestadores de serviço e operadores de dados;

VIII - Manter registro atualizado das operações de tratamento de dados pessoais, em conformidade com o art. 37 da LGPD;

IX - Elaborar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) sempre que o tratamento puder implicar alto risco aos direitos e liberdades fundamentais dos titulares, nos termos do art. 38 da LGPD;

X - Estabelecer que os servidores que tenham acesso a dados pessoais deverão, quando solicitados e dentro do prazo estipulado pela Secretaria de Administração deste Poder Legislativo, encaminhar o fluxo de tratamento desses dados, descrevendo de forma detalhada todas as etapas envolvidas, incluindo a coleta, o armazenamento, a utilização, o compartilhamento e a eliminação dos dados pessoais. As

informações fornecidas servirão de base para o mapeamento das atividades de tratamento realizadas por esta Casa Legislativa.

Art. 23 Nos casos de descarte, doação ou empréstimo de computadores e entre outros equipamentos que armazenem dados e documentos do Poder Legislativo de Jaru, é obrigatória a formatação, devendo ser encaminhado com antecedência para execução dos procedimentos.

Art. 24 O Poder Legislativo de Jaru, deve manter uma base de conhecimento com documentos que apresentam condutas e recomendações que melhoram o gerenciamento de risco e que orientam na tomada de ações adequadas em caso de comprometimento de dados pessoais.

Art. 25 Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deve ser comunicada a Autoridade Nacional de Proteção de Dados (ANPD) pelo Controlador, conforme artigo 48 da lei geral de proteção de dados.

CAPÍTULO VIII
DA POLÍTICA DE CONTROLE DE ACESSOS

Art. 26 Os vereadores e servidores deste Poder Legislativo com acesso ao sistema DigProc, bem como a quaisquer outros sistemas informatizados que contenham dados pessoais, deverão ter ciência e plena concordância com o Termo de Sigilo e Confidencialidade, conforme anexo II desta resolução. Tal termo estabelece a obrigação de manter a confidencialidade das informações acessadas, assegurando que o tratamento dos dados pessoais ocorra em conformidade com os princípios da segurança, da finalidade e da necessidade, previstos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Art. 27 O acesso a esses sistemas será restrito aos usuários devidamente autorizados, com perfis definidos de acordo com as atribuições funcionais, por meio de credenciais individuais usuário e senha e intransferíveis, sendo vedado o compartilhamento de credenciais ou o uso indevido das informações neles contidas.

Art. 28 Os perfis de acesso serão atribuídos conforme as funções institucionais exercidas, observando-se o princípio do acesso mínimo necessário. A revisão dos perfis será realizada periodicamente pela Secretaria de Administração, para assegurar a conformidade e o alinhamento com as funções de cada servidor ou agente político**.**

CAPÍTULO IX
DA POLÍTICA DE MONITORAMENTO

Art. 29 A Política de Monitoramento destina-se a estabelecer procedimentos e ações na segurança física/predial e manter a privacidade e segurança no uso de imagens capturadas pelo sistema de monitoramento das câmeras de segurança instaladas no âmbito deste Poder Legislativo, tendo como objetivos:

I Garantir a segurança dos vereadores, servidores, visitantes e terceiros;

II Prevenir e reprimir possíveis crimes;

III Proteger o patrimônio público;

IV Inibir práticas de vandalismo, depredação e uso indevido nas dependências;

V Monitorar áreas de acesso e circulação para fins de controle de fluxo;

VI Apoiar ações de fiscalização, auditoria e controle interno;

VII Auxiliar na apuração de incidentes, quando necessário, mediante requisição das autoridades competentes;

VIII Atuar de forma preventiva em situações de emergência, risco ou calamidade;

IX Auxiliar em investigações criminais e civis;

X Observar a legislação vigente sobre privacidade e proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados - LGPD;

XI Promover a transparência e a responsabilidade no uso das imagens coletadas, garantindo que sejam utilizadas estritamente para as finalidades institucionais.

§1º O monitoramento por câmeras de segurança será realizado unicamente para as finalidades de proteção do patrimônio público, segurança das autoridades, dos servidores, visitantes e terceiros, bem

como para a prevenção de atos ilícitos, não violando os direitos e liberdades fundamentais dos titulares dos dados previsto na Lei Geral de Proteção de Dados - LGPD.

§2º As imagens coletadas não poderão ser utilizadas para nenhuma outra finalidade além daquelas descritas no parágrafo anterior, sendo admitida sua transferência conforme o caso, somente pela Autoridade competente e em circunstâncias excepcionais, mediante determinação judicial ou investigação criminal. Ressalta-se que o sistema de videomonitoramento está instalado, prioritariamente, nas entradas, saguão, corredores e em pontos críticos de segurança das dependências da Câmara Municipal de Jaru, observando-se sempre os princípios da necessidade, proporcionalidade e transparência.

§3º Fica vedada a instalação de câmeras em banheiros e cozinha, sendo as câmeras posicionadas apenas em locais visíveis e devidamente identificados por placas informativas.

CAPÍTULO X
DAS CÂMERAS DE VIDEOMONITORAMENTO

Art. 30 O sistema de monitoramento público será composto pelos seguintes elementos:
I Câmeras de videomonitoramento estrategicamente instaladas em pontos de interesse público;
II Equipamentos e tecnologias complementares necessários à operação eficiente do sistema de monitoramento.
Art. 31 A instalação das câmeras de videomonitoramento observará critérios técnicos e objetivos, considerando:
I Estatísticas criminais oficiais;
II Vulnerabilidade de áreas estratégicas, como entradas, saídas e estacionamentos;
III Proteção do patrimônio público, incluindo bens móveis e imóveis;
IV Fluxo de veículos e pedestres;
V Áreas de maior circulação de pessoas;
VI Necessidade de segurança de autoridades, servidores, visitantes e terceiros;
VII Prevenção de atos de vandalismo, depredação ou uso indevido nas dependências deste Poder Legislativo;
VIII Condições de iluminação e visibilidade, de forma a assegurar a eficácia das imagens;
IX Atendimento às normas de privacidade e proteção de dados pessoais, nos termos da Lei Geral de Proteção de Dados - LGPD;
X Integração com outros sistemas de segurança e monitoramento eventualmente existentes.

CAPÍTULO XI
ACESSO, SOLICITAÇÃO E DIVULGAÇÃO DE IMAGENS DE VIDEOMONITORAMENTO

Art. 32 O acesso às imagens de videomonitoramento será regulado da seguinte forma: I Análise e encaminhamento: A análise inicial será realizada pela Secretaria de Administração, que poderá, conforme o grau de complexidade ou sensibilidade do pedido, encaminhá-lo ao(à) Presidente da Câmara Municipal para avaliação e decisão.

II Consentimento do titular:
Nos casos que envolvam dados pessoais sensíveis, o pedido será submetido previamente ao titular para obtenção de seu consentimento expresso. Após a autorização, as informações solicitadas serão disponibilizadas no prazo de até 15 (quinze) dias, em conformidade com a Lei nº 13.709/2018. Excepcionalmente, não será exigido o consentimento quando houver previsão legal específica ou determinação judicial que justifique a disponibilização das informações.

III Níveis de autorização para acesso: funções;

a) nível 1 Agentes de segurança pública e servidores públicos autorizados, no exercício de suas

b) nível 2 Pessoas físicas ou jurídicas que necessitem das imagens para investigação ou instrução processual, mediante requerimento formal aprovado pelo(a) Presidente do Poder Legislativo.

Art. 33 A solicitação de acesso às imagens classificadas como Nível 2 observará o seguinte procedimento:

I Requerimento:

O requerimento deverá ser apresentado junto à Câmara Municipal de Jaru, por meio de sistema eletrônico oficial, contendo:

a) Identificação completa do requerente, incluindo nome, CPF, RG, endereço, e-mail e contato atualizado;

b) Indicação precisa da data, horário e local da ocorrência, de forma exata ou aproximada;

c) Justificativa detalhada para o acesso solicitado;

d) Documentos comprobatórios que fundamentem o pedido, tais como boletim de ocorrência, ordem judicial, procuração específica ou outros necessários.

II Análise preliminar: A unidade administrativa responsável pelo monitoramento verificará a regularidade formal do requerimento.

III Encaminhamento para decisão: O pedido será encaminhado à autoridade competente no âmbito da Câmara Municipal, observados os princípios da legalidade, finalidade e proporcionalidade.

IV Registro e rastreabilidade: Todos os pedidos serão registrados em sistema próprio, assegurando rastreabilidade e transparência.

V Disponibilização das imagens:

Havendo aprovação, as imagens serão fornecidas exclusivamente por meio eletrônico, mediante envio seguro por e-mail institucional ou sistema de armazenamento em nuvem.

§1º O acesso será restrito ao intervalo de tempo especificado no requerimento, abrangendo somente o fato ocorrido que motivou a solicitação.

§2º As imagens só serão fornecidas mediante comprovação da necessidade, não podendo ser utilizadas para finalidades alheias às atribuições institucionais ou incompatíveis com as atividades de segurança e administrativas previstas nesta Resolução.

§3º É vedada a divulgação das imagens a terceiros, salvo autorização expressa do(a) Presidente da Câmara Municipal, observando-se que não será exigido o consentimento do titular quando houver previsão legal específica ou determinação judicial que justifique a disponibilização das informações.

Art. 34 Para investigações conduzidas por órgãos de segurança pública que demandem celeridade, as imagens poderão ser fornecidas mediante apresentação de ofício formal contendo identificação do órgão, do agente responsável, período e descrição do evento.

§1º O fornecimento será preferencialmente realizado em meio digital, mediante sistema eletrônico oficial.

§2º Excepcionalmente, quando houver inviabilidade técnica de disponibilização digital (tais como indisponibilidade temporária de sistemas, falha de conexão, volume excessivo de dados ou solicitação expressa da autoridade investigativa), as imagens poderão ser fornecidas em dispositivos físicos.

§3º Nesses casos, o fornecimento em dispositivo físico observará os seguintes procedimentos:

I Utilização de mídia oficial (como pen drive ou HD externo) devidamente lacrada e identificada;

II Emissão de termo de entrega contendo a descrição do conteúdo, número, ou identificação da mídia, data, horário e assinatura do responsável pelo recebimento;

III Adoção de medidas de segurança, como criptografia dos arquivos, sempre que tecnicamente viável.

§4º A Secretaria de Administração deverá abrir processo administrativo específico, no qual constarão todos os pedidos de requerimento, cópias dos ofícios, bem como os registros das imagens ou dados sensíveis eventualmente compartilhados.

CAPÍTULO XII
DA LGPD, SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Art.35 A operação do sistema de monitoramento público será realizada de forma ética, transparente e em conformidade com a Lei nº 13.709/2018 (LGPD), observando os direitos fundamentais dos cidadãos.

§1º. O acesso aos dados é restrito às finalidades previstas nesta Resolução.

§2º. Qualquer infração sujeitará o responsável a sanções administrativas, civis e criminais.
Art. 36 O acesso remoto ao sistema de videomonitoramento será controlado e limitado, garantindo que apenas servidores autorizados, previamente cadastrados e credenciados pela Secretaria de Administração, possam acessar as imagens ou dados sensíveis, respeitando os níveis de autorização previstos nesta Resolução.
Art. 37 O tratamento de dados observará bases legais específicas, com destaque para:
I Cumprimento de obrigação legal ou regulatória;
II Proteção da vida ou da incolumidade física do titular ou de terceiros;
III Garantia da segurança pública;
IV Investigação e repressão de infrações penais ou administrativas.
Art. 38 É expressamente vedada a divulgação, reprodução, compartilhamento ou qualquer forma de utilização das imagens captadas pelo sistema de monitoramento público por parte dos solicitantes de quaisquer níveis de acesso (Níveis 1 e 2) a meios de comunicação, redes sociais ou terceiros, incluindo imprensa televisiva, impressa, digital, ou perfis pessoais.
Art. 39 Todos os solicitantes de acesso às imagens, independentemente do nível, deverão obrigatoriamente assinar Termo de Confidencialidade e Responsabilidade, comprometendo-se a:
I Utilizar as imagens exclusivamente para os fins autorizados nesta Resolução;
II Não divulgar, reproduzir, compartilhar ou ceder as imagens a terceiros sem autorização expressa do(a) Presidente deste Poder Legislativo;
III Responder civil, administrativa e criminalmente por qualquer uso indevido das imagens.
Art. 40 O descumprimento das disposições dos artigos 38 e 39 implicará na imediata suspensão do acesso ao sistema de monitoramento e sujeitará o infrator às penalidades previstas na legislação aplicável, assegurados o contraditório e a ampla defesa.

CAPÍTULO XIII
AUDITORIA E CONFORMIDADE

Art. 41 O cumprimento desta Política, bem como dos normativos que a complementam, deverá ser avaliado periodicamente por meio de verificações de conformidade realizadas pela Controladoria desta Câmara, em conjunto com a Secretaria de Administração, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e a garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.
Parágrafo único. O relatório de avaliação de conformidade deve conter, no mínimo, as seguintes informações:
I - Data e horário da ação de verificação de conformidade;
II - Área ou setor auditado;
III - Procedimentos e instrumentos utilizados;
IV - Resultados da verificação;
V - Recomendações e ações corretivas
Art. 42 O descumprimento das normas e dos procedimentos referentes à proteção de dados pessoais, nos termos desta resolução e da legislação, poderá acarretar, isolada ou cumulativamente, a aplicação de sanções administrativas, civis e penais, assegurados o contraditório, a ampla defesa e o devido processo legal.

CAPÍTULO XIV
DISPOSIÇÕES FINAIS

Art. 43 As normas complementares de proteção de dados pessoais deverão abranger regras de boas práticas e de governança, estabelecendo os procedimentos e condições de organização e funcionamento, incluindo:
I Reclamações e petições de titulares;
II Normas de segurança e padrões técnicos;
III Obrigações específicas para os diversos envolvidos no tratamento;
IV Ações educativas e gerenciamento de riscos.

Art. 44 As diretrizes estabelecidas nesta Resolução não se esgotam em razão da contínua evolução tecnológica, alterações legislativas e do constante surgimento de novas ameaças e requisitos, podendo ser complementadas por outras medidas de segurança.

Art. 45 Esta Resolução será atualizada periodicamente, quando necessário, ouvido o Comitê Gestor de Proteção de Dados Pessoais CGPDP.

Art. 46 Integram esta Política Geral de Privacidade e Proteção de Dados Pessoais os seguintes anexos:

I Termo de consentimento para tratamento de dados pessoais;
II Termo de sigilo e confidencialidade;
III Procedimento para anonimização de dados.

Art. 47 Esta Resolução entra em vigor na data de sua publicação.

Tatiane de Almeida Domingues
Presidente

Silvio Aquerley da Silva
Vice-Presidente

Ademar Lopes do Nascimento
1º secretário

Celiandro Ribeiro de Jesus
2º Secretário

ANEXO I

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Pelo presente instrumento, os abaixo assinados, doravante denominados TITULARES, autorizam a Câmara Municipal de Jaru, inscrita no CNPJ sob o nº 05.705.900/0001-58, com sede na Rua Goiás, nº 3531, doravante denominada CONTROLADORA, a dispor de seus dados pessoais e dados pessoais sensíveis, tanto em meio físico quanto digital, em razão de vínculo trabalhista, fiscal e tributário, nos termos dos artigos 7º e 11 da Lei nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais, conforme cláusulas a seguir:

CLÁUSULA PRIMEIRA DADOS PESSOAIS TRATADOS

Os TITULARES autorizam a CONTROLADORA a realizar o tratamento dos seguintes dados pessoais e sensíveis, conforme aplicável a cada caso:

I Nome completo;
II Data de nascimento;
III Documentos oficiais com número e imagem (RG, CPF, CNH, PIS, Título de Eleitor, Certificado de Reservista, CTPS, Carteira Profissional, Diploma de Escolaridade, Certidões etc.);
IV Fotografia 3x4;
V Nome dos genitores;
VI Tipo sanguíneo e fator Rh;
VII Endereço, contatos telefônicos, WhatsApp e e-mail;
VIII Nome dos filhos e respectivos documentos;
IX Dados bancários (banco, agência, conta);
X Comunicação mantida entre titular e controlador;
XI Declarações e certidões exigidas para nomeação;
XII Exames e atestados médicos (admissionais, periódicos, de retorno, mudança de função etc.);
XIII Informações sobre estado civil e dependentes;
XIV Outros documentos exigidos por edital, Tribunal de Contas ou Estatuto dos Servidores.

CLÁUSULA SEGUNDA FINALIDADES DO TRATAMENTO

Os dados pessoais serão utilizados para as seguintes finalidades:

I Identificação e contato com o titular, em razão do vínculo empregatício;

II Cumprimento de obrigações legais, trabalhistas e previdenciárias;

III Admissão e execução do vínculo, inclusive após a exoneração;

IV Atendimento a obrigações impostas por órgãos fiscalizadores;

V Emissão de contracheques, recibos de pagamento, férias, 13º salário;

VI Requisições feitas pelo titular;

VII Exercício de direitos em processos judiciais e/ou administrativos;

VIII Proteção da vida ou da incolumidade física do titular ou de terceiros;

IX Atuação com base no interesse legítimo do controlador, quando aplicável;

X Contratação de serviços por interesse do titular (planos de saúde, bancos etc.);

XI Compartilhamento com sindicato ou associação de servidores.

CLÁUSULA TERCEIRA COMPARTILHAMENTO DE DADOS

A CONTROLADORA poderá compartilhar os dados com terceiros (inclusive órgãos públicos), desde que observados os princípios da boa-fé, finalidade, necessidade, segurança, transparência e demais dispostos na LGPD.

CLÁUSULA QUARTA SEGURANÇA DOS DADOS

A CONTROLADORA compromete-se a adotar medidas técnicas e administrativas para proteção dos dados pessoais, bem como comunicar à ANPD e aos titulares sobre incidentes de segurança, nos termos do art. 48 da LGPD.

CLÁUSULA QUINTA PRAZO DE TRATAMENTO

Os dados pessoais poderão ser tratados durante o vínculo com a Câmara Municipal de Jaru, e posteriormente, pelo tempo necessário para cumprimento de obrigações legais e auditorias, conforme art. 16 da LGPD.

CLÁUSULA SEXTA DIREITOS DOS TITULARES

Os TITULARES poderão, a qualquer tempo, mediante solicitação, exercer os seguintes direitos perante a CONTROLADORA:

I Confirmação da existência de tratamento de dados;

II Acesso aos dados tratados;

III Correção de dados incompletos, inexatos ou desatualizados;

IV Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos, ou tratados em desconformidade com a LGPD;

V Eliminação dos dados tratados com consentimento, salvo nas hipóteses previstas em lei;

VI Revogação do consentimento, a qualquer tempo, mediante solicitação por e-mail ou requerimento escrito, nos termos do §5º do art. 8º da LGPD.

CLÁUSULA SÉTIMA INCIDENTES DE SEGURANÇA

Em caso de vazamento de dados ou acessos não autorizados, as partes poderão firmar acordo quanto aos eventuais danos causados.

DECLARAÇÃO FINAL

Declaro(amos), para os devidos fins, que li(emos), compreendi(emos) e estou(amos) ciente(s) dos termos ora estabelecidos, consentindo expressamente com o tratamento dos meus/nossos dados pessoais e sensíveis para as finalidades descritas neste Termo.

ANEXO II

TERMO DE SIGILO E CONFIDENCIALIDADE

Declaro(amos), para os devidos fins, estar ciente(s) de que o acesso ao sistema DigProc, bem como a quaisquer outros sistemas informatizados que contenham dados pessoais, implica na responsabilidade de manter o sigilo e a confidencialidade das informações pessoais e institucionais ali contidas.

Comprometemo-nos a:

a) Utilizar os sistemas apenas para fins institucionais no estrito exercício das atribuições funcionais;

b) Não divulgar, compartilhar ou repassar a terceiros quaisquer informações pessoais ou dados sensíveis acessados;

c) Manter em absoluto sigilo as credenciais de acesso (login e senha), responsabilizando-me nos por sua guarda, uso adequado e não compartilhamento com terceiros;

d) Comunicar imediatamente à autoridade competente qualquer incidente de segurança, acesso indevido ou uso não autorizado de informações ou credenciais de acesso que vier a ser identificado;

e) Zelar pela integridade, disponibilidade e confidencialidade das informações acessadas, adotando boas práticas de segurança da informação no manuseio de dados;

f) Evitar o armazenamento de dados pessoais ou institucionais em dispositivos pessoais, mídias removíveis ou ambientes não autorizados, salvo quando expressamente permitido e com os devidos cuidados de segurança;

g) Não instalar, modificar ou utilizar softwares não autorizados nos sistemas institucionais, bem como não alterar configurações de segurança previamente estabelecidas;

Estou (amos) cientes de que o descumprimento das obrigações aqui assumidas poderá resultar em sanções administrativas, civis e penais, conforme a legislação vigente, em especial a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Por fim, declaro (amos) que a obrigação de manter confidencialidade sobre as informações a que tivermos acesso persiste mesmo após o término do vínculo funcional com o Poder Legislativo de Jaru.

ANEXO III

PROCEDIMENTOS PARA ANONIMIZAÇÃO DE DADOS

Exemplo de Aplicação do Método de Anonimização de Dados em Documentos para Publicação.	
TIPO DE DOCUMENTO	MÉTODO DE ANONIMIZAÇÃO
CPF	***.123.456 -**
RG	**123****
Demais documentos (endereço residencial e outros)	*****, cidade/UF
Estado Civil	******
Telefone	****123***
E-mail	usu*****@****.com
Data de nascimento	**1985
Nome da mãe	Nome suprimido
PIS/PASEP	***.***.***-**
Número da CNH	******123**
Placa de veículo	***-1234 ou suprimida
Dados bancários (banco, conta, agência)	Banco ***, ag. *** conta ***123
Nome completo (em casos de anonimato necessário)	Suprimido ou 'Pessoa Interessada'
Filiação (pai/mãe)	Informação suprimida

Tatiane de Almeida Domingues
Presidente

Silvio Aquerley da Silva
Vice-Presidente

Ademar Lopes do Nascimento
1º secretário

Celiandro Ribeiro de Jesus
2º Secretário

.

Documento assinado eletronicamente por **CELIANDRO RIBEIRO DE JESUS**, **VEREADOR**, em 15/12/2025 às 17:12, horário de JARU/RO, com fulcro no art. 14 da Resolução nº 265 de 14/02/2022.

Documento assinado eletronicamente por **SILVIO AQUERLEY DA SILVA**, **VEREADOR**, em 15/12/2025 às 17:15, horário de JARU/RO, com fulcro no art. 14 da Resolução nº 265 de 14/02/2022.

Documento assinado eletronicamente por **ADEMAR LOPES DO NASCIMENTO**, **VEREADOR**, em 16/12/2025 às 07:41, horário de JARU/RO, com fulcro no art. 14 da Resolução nº 265 de 14/02/2022.

Documento assinado eletronicamente por **TATIANE DE ALMEIDA DOMINGUES**, **Presidente do Poder Legislativo**, em 16/12/2025 às 08:20, horário de JARU/RO, com fulcro no art. 14 da Resolução nº 265 de 14/02/2022.

A autenticidade deste documento pode ser conferida no site eproc.jaru.ro.gov.br, informando o ID **3643378** e o código verificador **941157BD**.

Referência: Processo nº 51-545/2025. Docto ID: 3643378 v1