

QUEM FAZ O QUÊ?

TITULAR Pessoa natural a quem os dados se referem: cidadão, servidor, visitante, estagiário ou fornecedor pessoa física.	CONTROLADOR Organização que toma as principais decisões sobre a finalidade e os elementos essenciais do tratamento. Nas atividades institucionais: a Câmara.
OPERADOR Pessoa ou empresa que trata dados em nome do controlador, conforme instruções e contrato.	ENCARREGADO / DPO Canal entre Câmara, titulares e ANPD. Orienta, articula áreas e acompanha fluxos. Não decide no lugar do controlador.
COMITÊ Instância técnica, consultiva e de apoio à governança, à prevenção de riscos e à implementação da LGPD.	CADA UNIDADE Conhece suas rotinas, limita acessos, segue orientações, registra decisões e comunica riscos ou incidentes.

A responsabilidade é institucional. A execução é distribuída.

PRINCÍPIOS QUE VIRAM HÁBITOS

FINALIDADE Saiba por que o dado será utilizado.	ADEQUAÇÃO Use o dado de forma compatível com o contexto informado.
NECESSIDADE Colete, acesse e compartilhe apenas o mínimo.	TRANSPARÊNCIA Explique o tratamento com linguagem clara.
SEGURANÇA Proteja canais, sistemas, documentos e acessos.	PREVENÇÃO Pense no risco antes do envio, da publicação ou da contratação.
NÃO DISCRIMINAÇÃO Evite usos capazes de produzir exclusão ou tratamento abusivo.	RESPONSABILIZAÇÃO Registre decisões, controles e providências adotadas.
LIVRE ACESSO Facilita ao titular consultar como seus dados são tratados.	QUALIDADE DE DADOS Mantém os dados corretos, claros, relevantes e atualizados.

CONSENTIMENTO NÃO RESOLVE TUDO

A LGPD prevê várias hipóteses que autorizam o tratamento. No Poder Público, são frequentes o cumprimento de obrigação legal, o exercício de competências públicas, a execução de políticas públicas, o exercício regular de direitos, a proteção da vida e a tutela da saúde.

1 USE A BASE ADEQUADA

A base legal deve corresponder à finalidade real. Um termo de consentimento não corrige coleta excessiva, finalidade indefinida ou ausência de competência.

2 DADOS SENSÍVEIS

Possuem hipóteses próprias de tratamento e exigem proteção reforçada. O acesso deve ser estritamente necessário.

3 PODER PÚBLICO

O tratamento deve estar apoiado em hipótese legal adequada e atender à finalidade pública, ao interesse público e às competências legais, com informação clara sobre práticas e responsabilidades.

- Receba apenas os documentos necessários e explique a finalidade e o encaminhamento.
- Restrinja o acesso a dados sobre saúde, violência, renda, deficiência, crianças e outras vulnerabilidades.
- Use somente sistemas, processos, contas e canais institucionais autorizados. Não fotografe nem guarde documentos em celular, e-mail ou nuvem pessoal.
- Não use grupos de mensagens como arquivo permanente. Defina se o documento será juntado, guardado pelo prazo legal, devolvido ou descartado com segurança.

ATENDIMENTO AO CIDADÃO

URGÊNCIA EXIGE RAPIDEZ. NÃO AUTORIZA EXPOSIÇÃO AMPLA.

WHATSAPP E MENSAGENS

EVITE

RG, laudo ou lista em grupo amplo; prints com dados excessivos; uso do grupo como arquivo; backup em nuvem pessoal; números expostos em lista aberta.

FAÇA

Use canal institucional; limite destinatários; confira arquivo e conversa; transfira o registro necessário ao repositório oficial; utilize CCO quando contatos não precisarem ser revelados.

PROTEJA O APARELHO

Ative senha forte, autenticação em dois fatores, atualização, bloqueio automático e recursos de localização/apagamento quando autorizados.

ENVIO ERRADO

Tente conter ou revogar o acesso, preserve evidências e comunique imediatamente ao DPO e a Tecnologia, com ciência da chefia.

E-MAIL, PLANILHAS, PASTAS E ACESSOS

Use e-mail institucional e confira destinatários, domínio, anexos e conteúdo. Em mensagens coletivas, use CCO quando os destinatários não precisarem conhecer os contatos uns dos outros.

Evite “qualquer pessoa com o link” em arquivos que contenham dados pessoais. Conceda acesso por pessoa ou grupo funcional, com menor privilégio e prazo compatível. Revise permissões e remova acessos após desligamento, transferência ou encerramento da atividade.

Não esconda dados em abas, comentários ou colunas: remova-os da cópia que será compartilhada. Não envie a senha pelo mesmo canal do arquivo protegido. Use credenciais individuais. Senha compartilhada destrói a rastreabilidade. Bloqueie a tela ao se afastar e recolha documentos da impressora.

PUBLICAÇÃO, FOTOS E EVENTOS

Defina finalidade, base legal e público. Revise textos, anexos, assinaturas, QR Codes, metadados e nome do arquivo. Oculte dados excessivos e utilize tarjamento que elimine o conteúdo, não apenas o encubra.

Verifique telas, listas, crachás, documentos e endereços ao fundo de fotos e vídeos. Proteja a identidade e a vulnerabilidade de crianças. Não revele dados sensíveis por legendas. Separe inscrição, presença, certificação e comunicação futura, que possuem finalidades distintas.

TRANSPARÊNCIA, LAI E ANONIMIZAÇÃO

NEM OCULTAR TUDO, NEM PUBLICAR TUDO

A LGPD não revogou a Lei de Acesso à Informação. A resposta correta preserva a parte pública e restringe apenas o que estiver legalmente protegido.

VERSÃO PÚBLICA

Sempre que possível, forneça versão parcial, tarjada, minimizada ou anonimizada, com fundamentação da restrição.

ANONIMIZAÇÃO

O dado deve perder a possibilidade razoável de associação direta ou indireta a uma pessoa. Retirar o nome pode ser insuficiente.

CLASSIFICAÇÃO FORMAL

Informação pessoal restrita não se confunde com informação classificada em grau de sigilo. O TCI (termo de classificação de informação) é usado no procedimento próprio da LAI.

DADO PÚBLICO NÃO É DADO LIVRE PARA QUALQUER FINALIDADE.

ATIVIDADE INSTITUCIONAL & ELEITORAL

Mandato, partido e campanha podem se relacionar politicamente, porém não formam uma única base de dados. O cidadão que fornece telefone para atendimento institucional não autoriza, por isso, propaganda eleitoral.

Mantenha separação lógica e administrativa entre bases institucionais e eleitorais.

Não exporte contatos, demandas, listas de eventos ou perfis de vulnerabilidade da Câmara para campanha.

Não reutilize automaticamente imagem institucional em propaganda eleitoral ou finalidade pessoal.

Dados sobre opinião política e filiação partidária são sensíveis.

Não use recursos, sistemas ou contas institucionais para finalidade eleitoral indevida.

Diante de dúvida, suspenda a transferência e consulte o Encarregado e as áreas competentes.

INTELIGÊNCIA ARTIFICIAL E FERRAMENTAS DIGITAIS

NÃO COLE DADOS EM IA ABERTA

Não insira processos, laudos, listas, documentos pessoais, informações internas ou dados sensíveis em ferramentas abertas ou não contratadas institucionalmente.

FINALIDADE E CONTRATO

Ferramentas institucionais devem ter finalidade pública, base legal, segurança, minimização, cláusulas contratuais e avaliação de risco.

SUPERVISÃO HUMANA

Revise resultados, especialmente quando possam afetar direitos, produzir exposição ou orientar decisões administrativas.

DADOS PARA TREINAMENTO

Não utilize dados da Câmara para treinamento de modelos sem autorização formal, fundamento jurídico, contrato, avaliação de risco e ciência do DPO.

INCIDENTES: AGIR RÁPIDO E NÃO ESCONDER

Incidente não é apenas ataque hacker. Envio errado, link público, pasta perdida, celular roubado, acesso indevido, publicação acidental, alteração ou indisponibilidade também podem comprometer dados pessoais.

1

CONTENHA

Interrompa ou limite a exposição sem destruir evidências.

REGISTRE

Anote data, horário, sistemas, dados, titulares e providências.

2

3

COMUNIQUE

Avise imediatamente o DPO e a Tecnologia, com ciência da chefia.

COLABORE

Forneça as informações necessárias ao registro e à avaliação do risco.

4

5

NÃO IMPROVISE

Comunicação à ANPD, aos titulares ou à imprensa é decisão institucional do controlador.

PROTEÇÃO DE DADOS É BOM ATENDIMENTO

"Proteger dados não é proteger números. É proteger pessoas."

A Câmara recebe histórias, documentos e informações capazes de expor a intimidade, a segurança e os direitos dos cidadãos. A LGPD orienta como usar esses dados com legitimidade, necessidade, transparência e segurança. Ela não paralisa o trabalho: ajuda a fazê-lo melhor.

Antes de tratar um dado, faça seis perguntas:

PARA QUÊ?

Qual é a finalidade legítima e específica?

QUEM?

Quem realmente precisa acessar?

ATÉ QUANDO?

Há prazo de guarda ou descarte?

QUANTO?

Qual é o mínimo de dados necessário?

ONDE?

Em qual canal ou ambiente será guardado?

SE DER ERRADO?

Quem deve ser comunicado e como conter?

Se ninguém consegue responder, o processo precisa ser revisto.

DADO PESSOAL E DADO SENSÍVEL

DADO PESSOAL

Informação relacionada a uma pessoa natural identificada ou identificável. Exemplos: nome, telefone, e-mail, CPF, matrícula, imagem, voz, endereço IP e placa associável ao proprietário.

DADO PESSOAL SENSÍVEL

Categoria específica com proteção reforçada: origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados de saúde ou vida sexual, dados genéticos ou biométricos vinculados à pessoa.

TRATAMENTO

Toda operação com dados: receber, acessar, consultar, copiar, fotografar, enviar, compartilhar, publicar, guardar, alterar, arquivar ou eliminar.

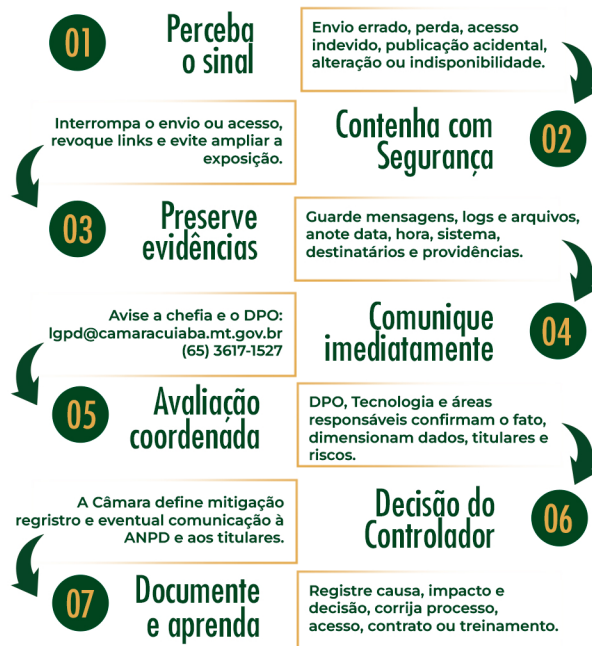
Retirar apenas o nome nem sempre impede a identificação.

Atenção: a LGPD protege dados de pessoas naturais. Documentos de empresas podem conter dados pessoais de sócios, representantes, empregados e contatos.

FLUXO DE COMUNICAÇÃO DE INCIDENTES

COM DADOS PESSOAIS

FLUXO INTERNO - SUSPEITA OU INCIDENTE COM DADOS PESSOAIS



PODE SER INCIDENTE:

E-mail ou WhatsApp enviado à pessoa errada.

Documento ou aparelho perdido, roubado ou descartado.

Link público, invasão ou acesso sem autorização.

Alteração, exclusão ou indisponibilidade de dados.

Publicação acidental de dados pessoais.

O QUE NÃO FAZER:

Não esconda nem espere "ver se alguém percebe".

Não apague evidências relevantes.

Não comunique externamente em nome da Câmara.

Não tente investigar acessando contas alheias.

Não amplie a exposição ao pedir ajuda em grupo aberto.

A PESSOA CONTINUA NO CENTRO DO TRATAMENTO. ENTRE OUTROS DIREITOS, PODE SOLICITAR:

- ATENDIMENTO FORMAL
DIREITOS DO TITULAR E CANAIS
- Confirmação da existência de tratamento e acesso aos dados;
 - Correção de informações incompletas, inexatas ou desatualizadas;
 - Informações sobre compartilhamentos e agentes envolvidos;
 - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou irregulares, observados os deveres de guarda;
 - Oposição, quando cabível, e informações sobre consentimento;
 - Revisão de decisões tomadas unicamente com base em tratamento automatizado, nos termos legais.



ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS
Hermes Teseu Bispo Freire Júnior
lgpd@camaracuiaba.mt.gov.br
(65) 3617-1527
camaracuiaba.mt.gov.br/lgpd

LGPD

NA PRÁTICA PARLAMENTAR



1. Colete somente o necessário.
2. Explique a finalidade.
3. Use canais institucionais.
4. Confira antes de enviar.
5. Não compartilhe senhas.
6. Restrinja e revise acessos.
7. Proteja dados sensíveis.
8. Separe atividade institucional e eleitoral.
9. Comunique incidentes imediatamente ao DPO e à Tecnologia.
10. Na dúvida, consulte o Encarregado antes de agir.

A LGPD não impede a atividade parlamentar. Ela organiza o uso responsável de dados pessoais.



CÂMARA MUNICIPAL DE CUIABÁ
SECRETARIA DE INFORMAÇÃO E TRANSPARÊNCIA