CIM AMUNESC

Consórcio Interfederativo Multifinalitário
da Região da Amunesc

Lei Federal nº 13.709/2018

LEI GERAL DE PROTEÇÃO DE DADOS

APRESENTAÇÃO

Nomes, CPFs, endereços, informações de saúde, dados de crianças tudo isso passa pelas mãos da administração pública. Com isso vem uma responsabilidade essencial: tratar essas informações com cuidado, respeito e segurança.

A Lei Geral de Proteção de Dados Pessoais (LGPD Lei nº 13.709/2018) estabelece as regras para esse tratamento. Ela se aplica tanto a empresas privadas quanto ao poder público, portanto, ao CIM-Amunesc e a cada município consorciado.

Esta cartilha é uma iniciativa do CIM-Amunesc para orientar os servidores e colaboradores do Consórcio na compreensão e aplicação da LGPD no cotidiano do serviço público. A proteção de dados deve chegar a todos, independentemente do cargo ou da área em que atuam.

Proteger dados pessoais é proteger pessoas. E isso é responsabilidade de todos nós

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

SUMÁRIO

1. Lei Geral de Proteção de Dados
1.1. O que é a LGPD?
1.2. Por que ela existe?
1.3. A quem a lei se aplica?
2. Conhecendo os Dados
2.1. Tipos de dados
3. Direitos dos Titulares
3.1. Quem é o Titular dos Dados?
3.2. Direito à Transparência e Acesso
3.3. Direito à Qualidade e Gestão
3.4. Direito de Contestação
4. Jornada dos Dados
4.1. Da Coleta à Eliminação
5. Agentes de Tratamento
5.1. Atribuições e Competências
6. Inteligência Artificial
6.1. O Que é Inteligência Artificial?
6.2. Uso Seguro com a LGPD
6.3. Os perigos das ferramentas Gratuitas
6.4. Regras para automação
7. Compartilhamento de Dados
7.1. Compartilhamento com Órgãos Públicos
7.2. Compartilhamento com Fornecedores
7.3. Acesso e Instruções do Controlador
7.4. Blindagem Jurídica com a LGPD
8. Gestão de Incidentes
8.1. Plano de Resposta Rápida
8.2. Protocolo de Ação
8.3. Deveres com a ANPD
9. Cultura de Privacidade e Boas Práticas
9.1. Zelo na Prática

LEI GERAL DE PROTEÇÃO DE DADOS

UNIDADE I

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

O QUE É A LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é a lei brasileira que regula o uso de informações pessoais de cidadãos. Ela define regras claras sobre como coletar, armazenar, usar e compartilhar dados de pessoas, tanto por empresas privadas quanto pelo poder público. A LGPD entrou em vigor em setembro de 2020 e representa uma mudança significativa na forma como a administração pública se relaciona com as informações dos cidadãos.

POR QUE ELA EXISTE?

Vivemos em um momento em que dados pessoais são gerados e coletados o tempo todo. Quando um cidadão solicita um benefício social, acessa um serviço de saúde, matricula um filho na escola ou entra em contato com a prefeitura, ele fornece informações pessoais. Essas informações, se mal utilizadas ou desprotegidas, podem causar danos sérios: exposição indevida da vida privada, discriminação e fraudes.

A LGPD existe para garantir que o tratamento de dados seja feito com respeito, transparência e segurança, e para assegurar que o cidadão tenha controle sobre as suas próprias informações.



A QUEM A LEI SE APLICA?

A LGPD se aplica a qualquer pessoa física ou jurídica, pública ou privada, que realize o tratamento de dados pessoais. No setor público, isso inclui prefeituras, secretarias, consórcios intermunicipais como o CIM-Amunesc, fornecedores contratados e todos os servidores e colaboradores. Em outras palavras: se no seu trabalho você coleta, consulta, armazena, compartilha ou descarta informações de cidadãos, a LGPD se aplica a você, independentemente do cargo ou da área em que atua.

Conhecer a LGPD não é opcional. É parte das suas responsabilidades como servidor/colaborador.

CONHECENDO OS DADOS

UNIDADE II

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

TIPOS DE DADOS

A LGPD trabalha com diferentes categorias de dados. Conhecê-las ajuda a identificar o nível de cuidado necessário em cada situação.

Dados Pessoais: Qualquer informação que identifique ou possa identificar uma pessoa. Por exemplo: nome, CPF, RG, endereço, telefone, e-mail, foto e matrícula funcional.

Dados Sensíveis: Exigem proteção reforçada pois podem gerar discriminação ou danos graves se expostos: origem racial ou étnica, convicção religiosa ou política, saúde, vida sexual, dados genéticos ou biométricos, filiação sindical.

Dados Anonimizados: São dados que passaram por um processo técnico que impede a identificação do titular. Quando devidamente anonimizados, saem do escopo da LGPD.

Dados Pseudonimizados: Dados que tiveram as informações de identificação substituídas por códigos ou pseudônimos. Ainda se enquadram na LGPD, pois a identificação pode ser revertida.

Dados de Crianças e Adolescentes: Recebem tratamento especial pela lei e exigem consentimento específico dos pais ou responsáveis, além de cuidados redobrados em todas as etapas do tratamento.

PRINCÍPIOS DA LGPD

UNIDADE III

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

OS 10 PRINCÍPIOS DA LGPD

Finalidade	Coletar dados apenas para objetivos legítimos e específicos.
Adequação	Os dados coletados devem ser compatíveis com a finalidade informada.
Necessidade	Coletar apenas o mínimo necessário. Quanto menos dados, menor o risco
Transparência	Informar ao cidadão como, por que e onde seus dados são usados.
Livre acesso	O cidadão tem o direito de consultar seus próprios dados a qualquer momento.
Qualidade	Mantenha os dados corretos, claros e atualizados.
Segurança	Proteger os dados contra acessos não autorizados, vazamentos e perdas.
Não discriminação	Dados pessoais não podem ser usados para prejudicar ou discriminar pessoas.
Prevenção	Adotar medidas para evitar danos antes que ocorram.
Responsabilização	Demonstrar que as boas práticas estão sendo efetivamente seguidas.

HIPÓTESES LEGAIS PARA O TRATAMENTO DE DADOS

UNIDADE IV

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

HIPÓTESES DE TRATAMENTO

Para tratar dados pessoais, não basta ter finalidade. É preciso ter amparo legal, ou seja, enquadrar o tratamento em uma das hipóteses previstas na LGPD.
No setor público, esse ponto é frequentemente mal compreendido: muitos servidores acreditam que precisam coletar o consentimento do cidadão para tudo, quando na verdade o poder público dispõe de hipóteses legais para fundamentar o tratamento de dados.

ART. 7º DA LGPD

O artigo 7º da LGPD lista dez hipóteses que autorizam o tratamento de dados pessoais. Veja cada uma delas:

CONSENTIMENTO DO TITULAR

Manifestação livre, informada, específica e inequívoca pela qual o titular concorda com o tratamento dos seus dados para uma finalidade determinada. No setor público, o consentimento é base residual: só deve ser usado quando nenhuma outra hipótese se aplicar, pois pode ser revogado a qualquer momento pelo titular.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA

Quando a lei ou regulamento impõe ao Consórcio a coleta ou o tratamento de determinados dados. O próprio texto normativo serve de amparo, dispensando consentimento. Exemplos: obrigações tributárias, registros de pessoal, prestação de contas a órgãos de controle. É uma das bases mais utilizadas pelo setor público.

EXECUÇÃO DE POLÍTICAS PÚBLICAS

Tratamento necessário para a execução de políticas públicas previstas em leis, decretos ou normas equivalentes, ou respaldadas em contratos, convênios e instrumentos similares. Aplica-se diretamente ao CIM-Amunesc, cujas ações interfederativas em educação, tributário, meio ambiente, planejamento e outros eixos se enquadram nessa hipótese.

REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA

Tratamento realizado por órgãos de pesquisa, garantida sempre que possível a anonimização dos dados pessoais. O uso dos dados deve ser exclusivo para a finalidade de pesquisa.

EXECUÇÃO DE CONTRATO OU PROCEDIMENTOS PRELIMINARES

Quando o tratamento é necessário para a execução de um contrato do qual o titular é parte, ou para procedimentos preliminares a pedido do titular. Aplica-se, por exemplo, ao tratamento de dados de fornecedores pessoa física contratados pelo Consórcio.

EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO

Tratamento necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Abrange o tratamento de dados em processos licitatórios, impugnações, recursos e defesas administrativas do Consórcio.

PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA

Tratamento indispensável para proteger a vida ou a incolumidade física do titular ou de terceiro. Hipótese aplicada em situações de emergência ou risco iminente.

TUTELA DA SAÚDE

Tratamento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária para procedimentos de saúde, inclusive assistência farmacêutica. Relevante para ações do Consórcio na área de saúde pública interfederativa.

INTERESSE LEGÍTIMO DO CONTROLADOR OU DE TERCEIROS

Tratamento necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto quando prevalecerem interesses ou direitos e liberdades fundamentais do titular. No setor público, essa base deve ser usada com cautela e fundamentação, pois o interesse legítimo não se confunde com conveniência administrativa.

PROTEÇÃO DO CRÉDITO

Tratamento necessário para a proteção do crédito, conforme legislação pertinente. Hipótese de aplicação mais restrita ao setor público, podendo ser relevante em operações financeiras do Consórcio.

HIPÓTESES PARA DADOS SENSÍVEIS

Dados sensíveis exigem amparo legal mais restrito. O art. 11 da LGPD lista as hipóteses aplicáveis, sendo as mais relevantes para o setor público:

ART. 11 DA LGPD

- **Consentimento específico e destacado do titular, para finalidades determinadas.**
- **Cumprimento de obrigação legal ou regulatória pelo controlador.**
- **Tratamento compartilhado de dados necessários à execução de políticas públicas, nos termos do inciso III do art. 7º.**
- **Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral.**
- **Proteção da vida ou da incolumidade física do titular ou de terceiro.**
- **Tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.**
- **Garantia da prevenção à fraude e à segurança do titular.**

Atenção: Tratar dados pessoais sem hipótese/base legal é uma violação da LGPD, mesmo que a intenção seja legítima. Em caso de dúvida sobre qual hipótese se aplica a uma situação específica, consulte o DPO ou a área jurídica do Consórcio.

DIREITO DOS TITULARES

UNIDADE III

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

QUEM É O TITULAR DOS DADOS?

O titular é a pessoa natural a quem os dados pertencem. É o cidadão que fornece suas informações ao buscar um serviço público, ao se cadastrar em um programa social, ao ser atendido em uma unidade de saúde ou ao interagir com qualquer órgão municipal. O titular tem direitos garantidos pela LGPD, e a administração pública tem a obrigação de respeitá-los.



No contexto do CIM-Amunesc, o titular pode ser:

- o cidadão atendido pelo Consórcio;
- o servidor público ou colaborador do Consórcio;
- qualquer pessoa física que tenha seus dados tratados pelo Consórcio, inclusive dados de cidadãos de municípios consorciados.
- o fornecedor pessoa física contratado pelo Consórcio.

DIREITO À TRANSPARÊNCIA E ACESSO

O titular dos dados tem o direito de saber quais informações a administração pública possui sobre ele, como elas são utilizadas, com quem são compartilhadas e qual é a finalidade do tratamento. O cidadão pode, a qualquer momento, solicitar ao Consórcio informações claras e completas sobre o uso dos seus dados pessoais.



DIREITO À QUALIDADE E GESTÃO

O titular tem o direito de exigir que seus dados estejam corretos, completos e atualizados. Informações desatualizadas ou incorretas podem prejudicar o cidadão, por exemplo, impedindo o acesso a um benefício ou gerando um atendimento inadequado.



DIREITO DE CONTESTAÇÃO

O titular tem o direito de contestar decisões tomadas com base no tratamento automatizado de seus dados pessoais, ou seja, decisões geradas por sistemas ou algoritmos sem intervenção humana direta, que afetem seus interesses.
No serviço público municipal, isso pode ocorrer em situações como análise automatizada de elegibilidade para programas sociais, triagem de beneficiários ou avaliações realizadas por sistemas digitais.

Dúvidas, informações sobre dados pessoais podem ser solicitadas por meio do formulário de ouvidoria, através do endereço eletrônico:

https://cimamunesc.sc.gov.br/formulario-ouvidoria/

JORNADA DOS DADOS

UNIDADE IV

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

DA COLETA À ELIMINAÇÃO

Coleta: Solicitar apenas os dados realmente necessários para a prestação do serviço. O cidadão deve saber quais dados estão sendo coletados e por quê.

Processamento: Os dados só podem ser tratados para a finalidade que motivou a coleta. Qualquer outro uso exige nova justificativa legal.

Compartilhamento: Dados pessoais só podem ser compartilhados com outros órgãos ou fornecedores quando houver amparo legal e necessidade justificada. Todo compartilhamento deve ser registrado.

Retenção: Os dados devem ser guardados pelo tempo estritamente necessário ou pelo prazo definido em lei. Manter dados além do necessário constitui violação da LGPD.

Eliminação: Quando os dados não forem mais necessários ou o prazo legal de guarda tiver encerrado, devem ser eliminados de forma segura, sem possibilidade de recuperação.

AGENTES DE TRATAMENTO

UNIDADE V

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

ATRIBUIÇÕES E COMPETÊNCIAS

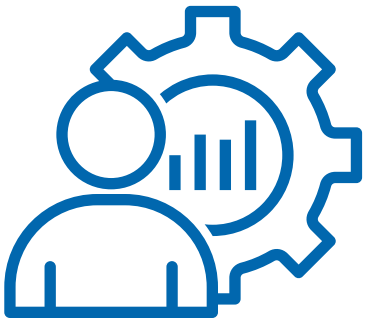
A LGPD define quem são os responsáveis pelo tratamento de dados. Esses responsáveis são chamados de agentes de tratamento e se dividem em duas figuras principais: o controlador e o operador.

CONTROLADOR



É quem decide como e por que os dados pessoais são tratados. No setor público municipal, o controlador é o próprio órgão público, a prefeitura, a secretaria ou o CIM-AMUNESC. É o controlador quem define as finalidades do tratamento e responde perante a lei e perante o cidadão.

OPERADOR



É quem trata os dados por conta do controlador, seguindo suas instruções. Podem ser operadores os fornecedores de sistemas, empresas terceirizadas ou qualquer prestador de serviço que acesse dados pessoais no exercício do contrato com o município ou com o Consórcio.

ENCARREGADO



É o profissional indicado pelo controlador para atuar como canal de comunicação entre o órgão público, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD). Sua indicação formal é obrigatória em todo órgão público que realize tratamento de dados pessoais.

INTELIGÊNCIA ARTIFICIAL

UNIDADE VI

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

O QUE É INTELIGÊNCIA ARTIFICIAL?



Inteligência Artificial (IA) é a capacidade de sistemas e programas de computador realizarem tarefas que normalmente exigiriam inteligência humana, como reconhecer padrões, tomar decisões, interpretar textos e imagens ou fazer previsões.

No serviço público municipal, a IA já está mais presente do que parece. Sistemas de triagem de beneficiários, chatbots de atendimento ao cidadão, ferramentas de análise de dados e plataformas de reconhecimento facial são exemplos de aplicações que utilizam inteligência artificial.

USO SEGURO COM A LGPD

Usar ferramentas de inteligência artificial, em especial, as generativas, no serviço público exige atenção à LGPD. São cuidados essenciais:

- Verificar se existe base legal para o tratamento dos dados que serão utilizados nas ferramentas de inteligência artificial generativa.
- Informar o cidadão quando uma decisão que o afeta for tomada com auxílio de algoritmos.
- Exigir garantias de segurança do fornecedor, em contrato.
- Certificar-se de que as ferramentas não geram tratamento discriminatório.
- Garantir sempre a possibilidade de revisão humana das decisões automatizadas.

OS RISCOS DAS FERRAMENTAS DE IA GENERATIVAS GRATUITAS

Ferramentas gratuitas de inteligência artificial disponíveis na internet, como assistentes de texto, tradutores automáticos e geradores de conteúdo, podem parecer práticas e inofensivas. Mas seu uso no serviço público exige atenção redobrada.

Ao inserir informações em uma ferramenta gratuita, o servidor/colaborador pode estar transmitindo dados pessoais de cidadãos para servidores de empresas privadas, muitas vezes localizadas fora do Brasil, sem qualquer garantia de segurança, sigilo ou conformidade com a LGPD.

COMPARTILHAMENTO DE DADOS

UNIDADE VII

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

COMPARTILHAMENTO COM ÓRGÃOS PÚBLICOS

No serviço público, é comum que diferentes órgãos precisem compartilhar informações para prestar serviços ao cidadão. A LGPD permite esse compartilhamento, mas estabelece condições claras para que ele ocorra de forma legal e segura.

QUANDO É PERMITIDO COMPARTILHAR?

O compartilhamento de dados entre órgãos públicos é permitido quando:

- existe finalidade legítima e específica para o tratamento;
- há amparo legal para o tratamento;
- existe necessidade real de acesso aos dados pelo órgão requerente.

É uma boa prática que o compartilhamento seja formalizado por meio de convênio, portaria, termo de cooperação ou outro instrumento legal adequado.

A formalização determina responsabilidades, prazos, acessos, tempo de armazenamento, quesitos de segurança da informação, dentre outros.

Os dados compartilhados devem se limitar ao estritamente necessário para a finalidade prevista, e todo compartilhamento deve ser registrado e rastreável.



O QUE NÃO É PERMITIDO?

Compartilhar dados pessoais de cidadãos informalmente, por e-mail pessoal, WhatsApp ou qualquer canal não oficial.

Fornecer dados a outro órgão sem verificar se existe amparo legal para isso.

Compartilhar mais dados do que o necessário para atender à finalidade.

COMPARTILHAMENTO COM FORNECEDORES

Quando o Consórcio contrata empresas para prestar serviços que envolvam acesso a dados pessoais de cidadãos ou servidores/colaboradores, essas empresas passam a atuar como operadoras de dados. Isso significa que elas também precisam cumprir a LGPD e que o Consórcio continua sendo responsável pelo tratamento realizado em seu nome.

O QUE DEVE ESTAR PREVISTO EM CONTRATO?

Todo contrato com fornecedor que envolva dados pessoais deve estabelecer, no mínimo:

- a obrigação de cumprir a LGPD;
- a finalidade e os limites do tratamento de dados;
- as medidas de segurança exigidas;
- a obrigação de comunicar incidentes ao Consórcio;
- a proibição de usar os dados para finalidade própria do fornecedor.
- tempo de acesso e retenção de dados, bem como a eliminação ou devolução ao final do contrato;
- sigilo e confidencialidade das informações acessadas;

ACESSO E INSTRUÇÕES DO CONTROLADOR

O controlador, que no setor público é o próprio órgão municipal ou o consórcio, é quem define as regras sobre como os dados pessoais devem ser tratados. Tanto os servidores/colaboradores quanto os fornecedores devem seguir essas instruções.

O QUE ISSO SIGNIFICA NA PRÁTICA?

O acesso aos dados pessoais deve ser concedido apenas a quem realmente precisa deles para exercer suas funções. Ninguém deve acessar, consultar ou utilizar dados pessoais além do que foi autorizado pelo controlador. Qualquer tratamento fora do que foi definido constitui violação da LGPD.

RESPONSABILIDADES DO CONTROLADOR:

- Definir quais dados podem ser tratados e por quem.
- Estabelecer os limites e as finalidades do tratamento.
- Garantir que servidores/colaboradores e fornecedores recebam as orientações necessárias.
- Monitorar o cumprimento das regras definidas.

RESPONSABILIDADES DE QUEM RECEBE ACESSO:

- Utilizar os dados apenas para a finalidade autorizada.
- Respeitar os limites definidos pelo controlador.
- Comunicar qualquer situação irregular ao DPO imediatamente.

BLINDAGEM JURÍDICA COM A LGPD

Cumprir a LGPD não é apenas uma obrigação legal. É também uma forma de proteger o Consórcio e o próprio servidor/colaborador de responsabilizações administrativas, civis e até penais decorrentes do mau uso de dados pessoais.



Órgãos públicos que demonstram adotar boas práticas de proteção de dados têm mais condições de se defender em caso de questionamentos, reclamações ou investigações da ANPD.
A documentação adequada dos processos, a realização de treinamentos e a existência de um DPO ativo são elementos que comprovam o compromisso institucional com a lei.

GESTÃO DE INCIDENTES

UNIDADE VIII

CIM AMUNESC
Consórcio Interfederativo Multifinalitário
da Região da AMUNESC

O QUE É UM INCIDENTE DE SEGURANÇA?

É qualquer evento que comprometa a confidencialidade, a integridade ou a disponibilidade de dados pessoais. Exemplos: vazamento de informações, acesso não autorizado a sistemas, perda de dispositivo com dados de cidadãos ou envio de dados para destinatário errado.
Um incidente de segurança pode acontecer mesmo nos órgãos públicos que adotam boas práticas. O que faz a diferença é a capacidade de identificar, comunicar e responder de forma rápida e organizada.



PLANO DE RESPOSTA RÁPIDA

Um incidente de segurança pode acontecer mesmo nos municípios que adotam boas práticas. O que faz a diferença é a capacidade de identificar, comunicar e responder de forma rápida e organizada.

PROTOCOLO DE AÇÃO

1. Identifique: Percebeu algo irregular? Não ignore. Qualquer suspeita de incidente deve ser tratada com seriedade.

2. Não tente resolver sozinho: Agir por conta própria pode agravar o problema e dificultar a investigação posterior.

3. Registre: Anote o máximo de informações: o que aconteceu, quando, quais dados podem ter sido afetados e quem teve acesso.

4. Comunique imediatamente: Informe seu superior e o DPO do órgão assim que possível. O tempo de resposta é fundamental.

5. Preserve as evidências: Não apague arquivos, registros ou históricos. Essas informações são essenciais para a apuração do incidente.

6. Aguarde orientação: Siga as instruções do DPO e da equipe responsável pela resposta ao incidente.

DEVERES COM A ANPD

A Agência Nacional de Proteção de Dados (ANPD) é o órgão federal responsável por fiscalizar o cumprimento da LGPD no Brasil. Municípios, Consórcios e todos os órgãos públicos têm deveres específicos perante a ANPD.

COMUNICAÇÃO DE INCIDENTES

Incidentes de segurança que possam causar risco ou dano relevante aos titulares devem ser comunicados à ANPD dentro de um prazo razoável. A omissão pode agravar as sanções aplicadas ao órgão.

COOPERAÇÃO COM A FISCALIZAÇÃO

Quando a ANPD solicitar informações, documentos ou esclarecimentos, o órgão público tem a obrigação de responder de forma completa e dentro do prazo estabelecido.

ELABORAÇÃO DE RELATÓRIOS

Em situações de tratamento de dados de alto risco, o Consórcio deve elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e disponibilizá-lo à ANPD quando solicitado.

DEVERES COM A ANPD

INDICAÇÃO DO DPO

Todo órgão público deve indicar formalmente um Encarregado de Tratamento de Dados e tornar suas informações de contato públicas e acessíveis, inclusive para a ANPD.

SANÇÕES APLICÁVEIS AO SETOR PÚBLICO

Diferentemente do setor privado, o poder público não está sujeito a multas financeiras pela ANPD. As sanções previstas para órgãos públicos são:

- Advertência com prazo para correção;
- Publicização da infração;
- Bloqueio dos dados envolvidos;
- Eliminação dos dados irregulares.

RESOLUÇÃO DE RECLAMAÇÕES

O cidadão pode registrar reclamações diretamente na ANPD quando sentir que seus direitos não foram respeitados pelo órgão público. A ANPD pode, então, instaurar processo administrativo e exigir resposta do órgão público.

BOAS PRÁTICAS COMO DEFESA

Órgãos Públicos que comprovam adotar boas práticas, como treinamentos, políticas internas e registros de tratamento, têm melhores condições de resposta perante a ANPD quando questionados.

CULTURA DE PRIVACIDADE E BOAS PRÁTICAS

UNIDADE IX

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc

ZELO NA PRÁTICA

A proteção de dados não depende apenas de sistemas ou políticas internas. Ela se constrói no dia a dia, com atitudes simples. Veja a seguir situações comuns e como agir corretamente em cada uma delas.

Recebeu um e-mail pedindo para atualizar cadastro ou clicar em link urgente? Desconfie. Sistemas oficiais nunca solicitam senhas por e-mail. Comunique o setor de TI (ou o gestor da área) antes de qualquer ação.



Vai imprimir um documento com dados de cidadãos? Fique próximo à impressora. Folhas esquecidas na bandeja podem ser vistas ou retiradas por qualquer pessoa que passar.



Vai compartilhar um documento com dados de cidadãos? Verifique antes se o destinatário tem autorização para receber aquelas informações. Enviar para a pessoa errada é um incidente de segurança.



Precisa tratar de assuntos do consórcio por e-mail? Nunca use e-mail pessoal para assuntos oficiais. Além de não ter validade oficial, você perde o controle sobre o destino das informações.



ZELO NA PRÁTICA

Veja situações do cotidiano e como agir corretamente em cada uma delas.

Atendeu um cidadão e precisa registrar informações? Use os sistemas oficiais do Consórcio. Bloquinhos, cadernos e papéis avulsos com dados pessoais são fontes de risco e não têm valor probatório.



Terminou o expediente? Verifique se não deixou documentos com dados pessoais sobre a mesa. Mesa limpa é também uma prática de proteção de dados.



Caso encontre, qualquer dispositivo móvel de armazenamento de dados, como um pen drive, ou hd externo sem identificação. Não conecte ao computador do Consórcio. Dispositivos desconhecidos podem conter vírus ou programas maliciosos.



Um colega pediu emprestado seu login e senha para acessar um sistema? Não empreste seu acesso a ninguém, nem a colegas de confiança. Tudo o que for feito com seu login é de sua responsabilidade.



CONSIDERAÇÕES FINAIS

Chegamos ao fim desta cartilha, mas o compromisso com a proteção de dados começa agora, no seu dia a dia como servidor público/colaborador.

A LGPD não é apenas uma exigência legal. É um reflexo de como a administração pública enxerga o cidadão: como titular de direitos, merecedor de respeito, transparência e segurança no tratamento das suas informações.

O CIM-Amunesc tem trabalhado para construir uma cultura de privacidade sólida e duradoura. Mas nenhuma política, sistema ou documento é suficiente sem o engajamento de cada servidor/colaborador.

Você é parte essencial dessa construção. Proteger dados pessoais é proteger pessoas. E essa confiança se constrói com atitudes simples, tomadas todos os dias.

FICHA TÉCNICA

TITULO:
Lei Geral de Proteção de Dados no CIM-Amunesc

ELABORAÇÃO:
Colaboração de Danielly Caroline H. A. J. Werneck de Carvalho - Estagiária de Direito da Área de Proteção de Dados do Município de Joinville

COORDENAÇÃO GERAL:
Sahmara Liz Botemberger - Encarregada pelo Tratamento de Dados Pessoais

Versão 1.0
2026

CIM Amunesc
Consórcio Interfederativo Multifinalitário
da Região da Amunesc