DECRETO Nº 3.108 DE 28 DE JULHO DE 2022

"Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta"

REGINA HELENA JANIZELO MORAES, Prefeita do Município de Águas da Prata - (Estância Hidromineral), Estado de São Paulo, no uso de suas atribuições legais, e

D E C R E T A:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º - Este decreto regulamenta a Lei Federal nº 13.709, de 14 de agosto de 2018, Lei de Proteção de Dados Pessoais (LGPD), no âmbito do Poder Executivo Municipal, estabelecendo competências, procedimentos e providências correlatas a serem observados por seus órgãos e entidades, visando garantir a proteção de dados pessoais.

Art. 2º - Para os fins deste decreto, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais em suporte eletrônico ou físico;

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

VI - controlador: pessoal natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

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

XIII - plano de adequação: conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais.

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

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI – transparência: garantia aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – prevenção: adoção de medidas para prevenir a ocorrência de dados em virtude do tratamento de dados pessoais;

IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II
DAS RESPONSABILIDADES
DAS RESPONSABILIDADES NA ADMINISTRAÇÃO PÚBLICA MUNICIPAL DIRETA

Art. 4º - O Poder Executivo Municipal, por meio de suas Secretarias e Subprefeitura, nos termos da Lei Federal nº 13.709, de 2018, deve realizar e manter continuamente atualizados:

I – o mapeamento dos dados pessoais existentes e dos fluxos de dados pessoais em suas unidades;

II – a análise de risco;

III – o plano de adequação, observadas as exigências deste Decreto e da Lei 13.708/2018;

IV – o relatório de impacto à proteção de dados pessoais, quando solicitado.

Parágrafo Único - Para fins do inciso III do "caput" deste artigo, as Secretarias e Subprefeitura devem observar as diretrizes editadas pela Controladora.

Art. 5º - Fica designada Bruna Luísa Anadão como a encarregada da proteção de dados pessoais, para os fins do art. 41 da Lei Federal nº 13.709, de 2018, nos moldes de contratação terceirizada.

§ 1º - A identidade e as informações de contato da encarregada estão disponíveis no site da Prefeitura, em seção específica sobre tratamento de dados pessoais, podendo ser acessados através do link: https://www.aguasdaprata.sp.gov.br/lgpd.php

§ 2º - O canal de atendimento específico para tal assunto se faz através do e-mail: protecaodedados@aguasdaprata.sp.gov.br

Art. 6º - São atribuições do encarregado da proteção de dados pessoais:

I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações da autoridade nacional e adotar providências;

III – orientar os funcionários e os contratados da Administração Pública Direta a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV – editar diretrizes para a elaboração dos planos de adequação, conforme art. 4º, inciso III deste Decreto;

V – opinar sobre as sugestões formuladas pela autoridade nacional a respeito da adoção de padrões e de boas práticas para o tratamento de dados pessoais, nos termos do art. 32 da Lei Federal nº 13.709, de 2018;

VI– providenciar a publicação dos relatórios de impacto à proteção de dados pessoais previstos pelo art. 32 da Lei Federal nº 13.709, de 2018;

VII - recomendar a elaboração de planos de adequação relativos à proteção de dados pessoais ao encarregado das entidades integrantes da Administração indireta, informando eventual ausência à Secretaria responsável pelo controle da entidade, para as providências pertinentes;

VIII - providenciar, em caso de recebimento de informe da autoridade nacional com medidas cabíveis para fazer cessar uma afirmada violação à Lei Federal nº 13.709, de 2018, nos termos do art. 31 daquela lei, o encaminhamento ao órgão municipal responsável pelo tratamento de dados pessoais, fixando prazo para atendimento à solicitação ou apresentação das justificativas pertinentes;

IX - avaliar as justificativas apresentadas para o fim de:

a)- caso avalie ter havido a violação, determinar a adoção das medidas solicitadas pela autoridade nacional;

b)- caso avalie não ter havido a violação, apresentar as justificativas pertinentes à autoridade nacional, segundo o procedimento cabível.

X - requisitar das Secretarias e Subprefeitura responsáveis as informações pertinentes, para sua compilação em um único relatório, caso solicitada pela autoridade nacional a publicação de relatórios de impacto à proteção de dados pessoais, nos termos do artigo 32 da Lei Federal nº 13.709, de 2018;

XI – executar as demais atribuições estabelecidas em normas complementares.

Parágrafo Único - Na qualidade de encarregada da proteção de dados, a Encarregada de Dados do Município está vinculada à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com a Lei Federal nº 13.709, de 2018 e com a Lei Federal nº 12.527, de 2011.

Art. 7º - Cabe ao Secretário de Gabinete da Controladora:

I – dar cumprimento, no âmbito dos respectivos órgãos, às recomendações do encarregado de proteção de dados pessoais;

II - atender às solicitações encaminhadas pelo encarregado de dados, no sentido de fazer cessar uma afirmada violação à Lei Federal nº 13.709, de 2018, ou apresentar as justificativas pertinentes;

III – encaminhar ao encarregado, no prazo por este fixado:

a) - informações sobre o tratamento de dados pessoais que venham a ser solicitadas pela autoridade nacional, nos termos do art. 29 da Lei Federal nº 13.709, de 2018;

b) - informações necessárias à elaboração de relatórios de impacto à proteção de dados pessoais, nos termos do art. 32 da Lei Federal nº 13.709, de 2018.

IV - assegurar que o Controlador Geral do Município seja informado, de forma adequada, a partir da ciência de eventual ocorrência de incidente de segurança, de todas as questões relacionadas com a proteção de dados pessoais no âmbito do Poder Executivo municipal.

Art. 8º - Caberá aos servidores públicos municipais, empregados públicos e ocupantes de cargo em comissão, bem como aos terceiros contratados que por ventura exerçam atividades relacionadas ao tratamento de dados pessoais:

I- Cumprir com as disposições trazidas na Lei Geral de Proteção de Dados, Lei n. 13.709/18 e a realizar o tratamento de dados em observação aos princípios e fundamentos desta;

II- Informar o encarregado de dados de forma escrita (e-mail ou notificação interna) eventuais comprometimentos à base de dados, na data do conhecimento do evento;

III- Guardar sigilo sobre os dados e informações pessoais a que tiver acesso em função do exercício de suas atividades, sob pena de ser responsabilizado juridicamente em caso de exposição indevida, desonesta, humilhante e/ou fraudulenta;

IV- Não divulgar informações pessoais contidas nos dispositivos eletrônicos que utilizarem, exceto se tais dados forem necessários para o exercício de suas funções contratadas;

V- Estar ciente que, caso necessário, sua caixa de e-mail para uso corporativo poderá ser acessada, não tendo razoável expectativa de privacidade quanto a esta;

VI - Não empregar de forma intencional nenhum tipo de ameaça interna junto a rede corporativa, recursos e dados confidenciais do Município, tais como:

a) Tratar erroneamente os dados confidenciais;
b) Ameaçar as operações de servidores internos ou de dispositivos de infraestrutura de rede;
c) Facilitar ataques externos conectando mídias USB infectadas no sistema de computador corporativo;
d) Convidar acidentalmente malware para a rede por e-mail ou sites mal-intencionados;
e) Utilizar de e-mail corporativo para spam ou promoção de negócios pessoais;
f) Instalar ferramenta não autorizada;
g) Utilizar de pendrive de forma não autorizada;
h) Imprimir documentos de forma não autorizada;
i) Realizar má utilização de um sistema;
j) Obstruir a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não se comunicarem adequadamente.

VII - Praticar suas condutas diárias de acordo com o estabelecido neste Decreto, bem como na Cartilha de Boas Práticas que se encontra anexa;

VIII – Fomentar e contribuir para o desenvolvimento e implantação da cultura inerente a proteção de dados;

IX – Saber direcionar as demandas ou pedidos dos titulares para o encarregado de dados, conforme disposto neste Decreto.

Art. 9º - Conforme disposto na Lei 13.709/2018 (LGPD), será garantido aos titulares de dados:

I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709, de 2018;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei 13.709, de 2018;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do §5º do art. 8º da Lei 13.709, de 2018.

§ 1º - O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º - O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei 13.709, de 2018.

§ 3º - Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º - Em caso de impossibilidade de adoção imediata da providência, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º - Havendo solicitação pelo titular inerente aos seus direitos, as partes comprometem-se a atender ao pedido de imediato, quando possível, no prazo de 15 (quinze) dias, sob justificativa, de forma gratuita.

CAPÍTULO III
DO TRATAMENTO DE DADOS PESSOAIS PELA ADMINISTRAÇÃO PÚBLICA MUNICIPAL

Art. 10 - O tratamento de dados pessoais pelos órgãos e entidades da Administração Pública Municipal deve:
I - objetivar o exercício de suas competências legais ou o cumprimento das atribuições legais do serviço público, para o atendimento de sua finalidade pública e a persecução do interesse público;
II - observar o dever de conferir publicidade às hipóteses de sua realização, com o fornecimento de informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a sua execução.

Art. 11 - Os órgãos e as entidades da Administração Pública Municipal podem efetuar o uso compartilhado de dados pessoais com outros órgãos e entidades públicas para atender a finalidades específicas de execução de políticas públicas, no âmbito de suas atribuições legais, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da Lei Federal nº 13.709, de 2018.

Art. 12 - É vedado aos órgãos e entidades da Administração Pública Municipal transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei Federal nº 12.527, de 2011;
II - nos casos em que os dados forem acessíveis publicamente, observadas as disposições da Lei Federal nº 13.709, de 2018;
III - quando houver previsão legal ou a transferência for respaldada, por meio de cláusula específica, em contratos, convênios ou instrumentos congêneres, cuja celebração deverá ser informada pelo responsável ao Controlador Geral do Município para comunicação à autoridade nacional de proteção de dados;
IV - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Parágrafo Único - Em quaisquer das hipóteses previstas neste artigo:

I - a transferência de dados dependerá de autorização específica conferida pelo órgão municipal à entidade privada;

II - as entidades privadas deverão assegurar que não haverá comprometimento do nível de proteção dos dados garantido pelo órgão ou entidade municipal.

Art. 13 - Os órgãos e entidades da Administração Pública Municipal podem efetuar a comunicação ou o uso compartilhado de dados pessoais a pessoa de direito privado, desde que:

I – o Encarregado de Dados informe a Autoridade Nacional de Proteção de Dados, na forma do regulamento correspondente;

II - seja obtido o consentimento do titular, salvo:

a)- nas hipóteses de dispensa de consentimento previstas na Lei Federal nº 13.709, de 2018;

b)- nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do art. 10, inciso II deste decreto;

c)- nas hipóteses do art. 12 deste decreto.

Parágrafo Único - Sempre que necessário o consentimento, a comunicação dos dados pessoais a entidades privadas e o uso compartilhado entre estas e os órgãos e entidades municipais poderão ocorrer somente nos termos e para as finalidades indicadas no ato do consentimento.

Art. 14 - Os planos de adequação devem observar, no mínimo, o seguinte:

I – publicidade das informações relativas ao tratamento de dados junto ao site do Município;

II – atendimento das exigências que vierem a ser estabelecidas pela Autoridade Nacional de Proteção de Dados, nos termos do art. 23, § 1º, e do art. 27, parágrafo único da Lei Federal nº 13.709, de 2018;

III – manutenção de dados em formato interoperável e estruturado para o uso compartilhado de dados com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 15 - As entidades integrantes da Administração Municipal indireta que atuarem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, deverão observar o regime

relativo às pessoas jurídicas de direito privado particulares, exceto quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, nos termos do art. 24 da Lei nº 13.709, de 2018.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 16 - A Prefeitura Municipal de Águas da Prata, na qualidade de Controladora de Dados, informa que para cada Secretaria integrante está sendo criada Políticas de Privacidade a fim de registrar o fluxo de tratamento de dados pessoais.

Art. 17 - Quanto ao tratamento de dados inerentes aos servidores municipais, informa-se que a Política de Privacidade está disponível para Consulta junto ao Departamento de Recursos Humanos ou no sítio eletrônico.

Art. 18 - Também serão disponibilizadas as Políticas de Privacidade de cada um dos Departamentos que compõem a atual Administração. Tais materiais poderão ser consultados junto ao sítio eletrônico do Município.

Art. 19 - Este decreto entrará em vigor na data de sua publicação.

Município de Águas da Prata – SP (Estância Hidromineral), aos vinte e oito do mês de julho de dois mil e vinte e dois.

Regina Helena Janizelo Moraes
Prefeita Municipal

2021

CARTILHA DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS E PRIVACIDADES.

PREFEITURA MUNICIPAL ÁGUAS DA PRATA.

BRUNA LUÍSA ANADÃO.

B2L.ADV

28/05/2021

1 – Identificação do Propósito do Tratamento e Minimização dos Dados na Coleta

A identificação da finalidade do tratamento de dados pessoais serve, fundamentalmente, para que as operações do ciclo de vida do dado sejam realizadas em conformidade com as regras estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Dessa maneira, o servidor municipal deve identificar o propósito de cada tratamento que pretenda realizar antes mesmo do Início desse tratamento, verificando qual a base legal adequada para o desenvolvimento dessa finalidade e se os dados a serem coletados são os estritamente necessários para o cumprimento desse propósito.

Na proteção de dados e da privacidade, menos é mais, pois, conforme o princípio da necessidade, a coleta de dados deve se dar de maneira restritiva, sempre limitada, portanto, ao propósito previamente estabelecido.

2 - Transparência e Lealdade no Tratamento de Dados Pessoais

O tratamento de dados pessoais deve ser realizado pelo servidor municipal sempre de forma lícita, transparente e garantindo a lealdade desse processamento para com os cidadãos cujos dados pessoais estão sendo tratados. Dessa forma, na medida em que se assegura a privacidade dos dados pessoais, se exige mais transparência quanto às atividades do tratamento, que deve ser sempre realizado em consonância com o ordenamento jurídico e em conformidade com a finalidade inicialmente comunicada aos cidadãos.

O servidor municipal não pode utilizar os dados pessoais para outras finalidades que não sejam compatíveis com o propósito original apresentado antes da coleta dos dados, devendo, igualmente, garantir aos cidadãos que seus dados pessoais sejam conservados apenas durante o tempo necessário às finalidades para as quais foram recolhidos.

Por fim, os dados pessoais não podem ser coletados senão para finalidades específicas, sendo vedada a coleta para fins indefinidos.

3- Promoções dos Direitos e Garantias dos Titulares de Dados.

O servidor municipal deve sempre realizar as atividades de tratamento de dados pessoais respeitando e priorizando os direitos e garantias dos cidadãos. Dessa maneira, deve imprimir os mais variados esforços para garantir que os titulares de dados sejam corretamente atendidos quando realizarem requisições.

Como as de retificação e de atualização de seus dados, bem como deve ser garantida aos cidadãos a possibilidade de revogação de seu consentimento nos tratamentos em que esse for solicitado.

Além disso, o servidor municipal deve garantir aos cidadãos informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, assegurando, também, a impossibilidade de realização do Tratamento para fins discriminatórios, ilícitos ou abusivos.

Portanto, são direitos dos cidadãos, enquanto titulares de dados, informação sobre o tratamento, eventuais compartilhamentos, as condições do consentimento, quando for o caso, e a possibilidade de sua revogação.

4- Anonimização e Pseudonimizaçãodos Dados Pessoais

O servidor municipal deve utilizar os meios técnicos razoáveis e disponíveis no momento do tratamento, para garantir, sempre que necessário, a manutenção da privacidade do cidadão, a anonimização ou pseudonimização dos dados pessoais, situações empregadas para que o dado perca, permanentemente ou temporariamente, a possibilidade de associação, direta ou indireta, a um indivíduo.

A pseudonimização é o tratamento de dados pessoais que garante que tais dados não possam mais ser atribuídos ao titular de dados sem o uso de informações adicionais. Na pseudonimização, os dados permanecem como dados pessoais.

Por sua vez, a anonimização é o tratamento de dados pessoais que garantem que os dados não possam mais ser atribuídos ao titular de dados de forma alguma. Os dados pessoais que passam pelo processo de anonimização se tornam dados estatísticos.

5- Consentimento

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados Pessoais para uma finalidade determinada. Nesse sentido, caso o consentimento seja coletado para o tratamento dos dados pessoais, deve-se garantir que todos seus requisitos sejam cumpridos.

Além disso, o servidor municipal deve garantir instrumentos controles para gerenciar a concessão ou revogação do consentimento pelo cidadão.

O consentimento explícito é necessário para o tratamento de dados pessoais sensíveis: origem racional ou étnica, dados genéticos ou biométricos, filiação política, religiosa ou filosófica, dado referente à saúde ou a vida sexual, opinião política, filiação sindical e convicção religiosa.

6- **Avaliações do Risco**

O servidor municipal deve realizar o diagnóstico dos processos de tratamento dos dados pessoais, identificando os riscos envolvidos na atividade.

Compreendendo a importância da mitigação desses riscos para evitar incidentes de segurança, o servidor municipal deve elaborar um plano de conformidade do processamento de dados, contendo: a descrição do risco (área de ocorrência, atividade afetada e evento de risco), a avaliação do risco eminente (probabilidade, impacto, nível de risco inerente), a avaliação do risco residual (controles existentes, avaliação do controle, nível de risco residual) e o plano de resposta ao risco (tipo de tratamento, medidas de tratamento, responsável pela implementação das medidas).

7- **Compartilhamentos dos Dados Pessoais**

O compartilhamento de dados pessoais somente deve ocorrer.

Quando consentâneo com a finalidade do tratamento desses dados. Em algumas situações, é necessário, inclusive, o consentimento do titular de dados para que esse compartilhamento seja permitido, obedecidos os requisitos legais.

Dessa mesma forma, é obrigação do servidor municipal não compartilhar documentos com os dados pessoais dos cidadãos por e-mail, nuvens não

homologadas pela PMSP e, especialmente, por aplicativos de comunicação instalados nos celulares funcionais ou pessoais.

8 - Treinamento e Comunicação

O estabelecimento de uma cultura de proteção de dados e privacidade é indispensável para o desenvolvimento do tratamento de dados baseado nos princípios da Lei Geral de Proteção de Dados.

O servidor municipal deve sempre buscar o aprimoramento de sua capacidade decisória quanto as atividades envolvidas no tratamento de dados pessoais por meio de capacitações relacionadas com o tema. Além disso, deve se colocar como agente promotor das boas práticas de proteção de dados e privacidade no ambiente da sua unidade, incentivando os demais colaboradores a realizarem suas atividades também em conformidade com essas boas práticas.

9 - Resposta a Incidentes de Segurança.

As boas práticas de proteção de dados e privacidade também exigem do servidor municipal prontidão no atendimento a incidentes de seguranças. Vazamentos de dados pessoais, co-rompimento do banco de dados, utilização de ferramenta não autorizada, ou até mesmo documentos contendo dados pessoais esquecidos na impressora devem ser considerados incidentes de seguranças e ser tratados pelos servidores municipais de forma séria e diligente.

Todos os esforços para responder ao incidente devem ser adotadas, especialmente a transparência na comunicação ao superior hierárquico, a chefia de gabinete (nos termos do art. 7º do Decreto (Nº 59.767) e ao titular de dados pessoais

10- Monitoramento

O servidor municipal deve monitorar se todas as regras, políticas, processos e procedimentos estão sendo observados nas atividades de tratamento de dados pessoais, garantindo, assim o cumprimento das garantias e direitos dos titulares desses dados.

Além disso, deve sempre buscar, no monitoramento, uma forma de promoção de melhorias nas suas atividades de tratamento de dados pessoais, corrigindo erros e inconsistências que venha a detectar por meio desse monitoramento.

11- Interpretação

A privacidade é o uso adequado dos dados. Quando as administrações públicas coletam informações fornecidas pelos cidadãos ou funcionários, elas devem usar esses dados apenas para a finalidade a que se designam.

12- CONDUTAS RECOMENDADAS / BOAS PRÁTICAS

- Conhecer os direitos dos titulares e saber direcioná-lo ao encarregado que poderá atende-lo sobre o aspecto do tratamento de dados pessoais;
- POLÍTICA DA TELA BLOQUEADA + POLÍTICA DA MESA LIMPA.
- Utilizar antivírus em suas máquinas;
- Utilizar Senhas Fortes / Trocar de Senha Periodicamente;
- Sugerir medidas que possam contribuir para a proteção de dados pessoais da sua empresa, do seu Setor.
- Ler as Políticas de Privacidade e Termos de uso dos Sites.

Afinal o que são termos de Uso e Política de Privacidade?

Os **Termos e Condições** indicam as regras que devem ser respeitadas ao se fazer uso do site e podem prevenir eventuais reclamações dos usuários.

A **Política de Privacidade de Dados** é utilizada para informar aos usuários do site como suas informações pessoais serão coletadas, armazenadas e compartilhadas com outros parceiros ou vendidas para outras empresas.

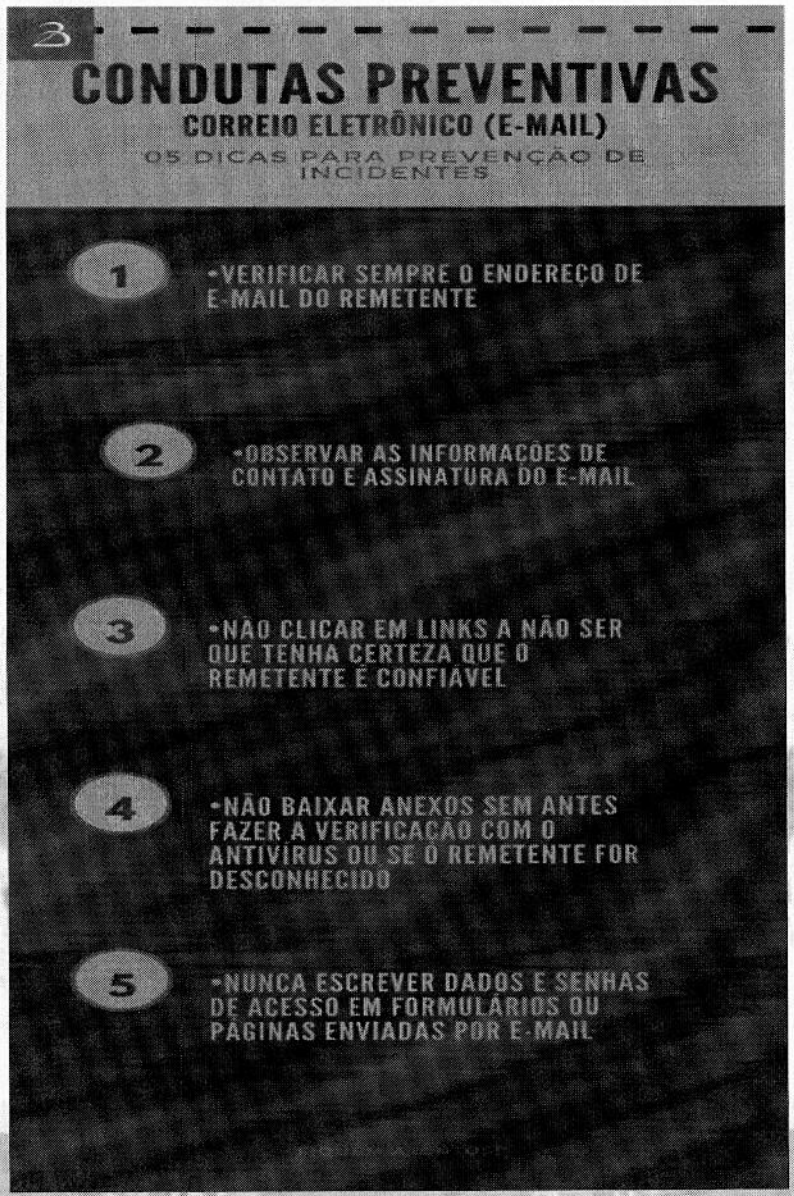
"Termo de Uso" e a "Política de Privacidade" são **contratos eletrônicos** que visam limitar a responsabilidade, direcionar a forma de utilização do seu produto/serviço por parte dos clientes, assim como esclarecer possíveis dúvidas que seu cliente tenha sobre o funcionamento do seu serviço/produto.

Tais documentos são **contratos de adesão** (significa que há imposição dos termos e condições aos clientes), portanto, devemos entender que para que esses documentos tenham validade jurídica precisamos estabelecer as cláusulas de modo coerente e sem abusividade.

Obs.: As vítimas comuns incluem sistemas desatualizados ou sem detecção de vírus e spam.

13- PECULIARIDADES SOBRE A UTILIZAÇÃO DO E-MAIL

Com o intuito de prevenir incidentes relacionados à utilização do correio eletrônico, sugerimos as seguintes condutas a serem adotas:



Atenção: Direito à Privacidade sobre caixas de e-mail corporativas.

13.1 Do Direito à privacidade na utilização de e-mail

O Poder Judiciário através do julgamento de casos, entende que o direito à privacidade não se aplica sobre a caixa de e-mail referente a conta corporativa. Portanto, havendo algum incidente que careça de acesso ao e-mail pelo órgão ou empresa, estes poderão acessá-los sem qualquer objeção.

13.2 Como identificar e-mail suspeito

Os golpistas tentam copiar e-mails e mensagens de texto de empresas legítimas para enganar você e obter senhas e informações pessoais. Estes sinais podem ajudar a identificar fraudes:

- O endereço de e-mail ou telefone do remetente não correspondem ao nome da empresa a qual ele alega pertencer.
- O endereço de e-mail ou telefone usados para entrar em contato com você não são os mesmos que você informou à empresa.
- Um link em um e-mail parece correto, mas o URL não corresponde ao site da empresa.
- O e-mail é bem diferente dos outros que você já recebeu da empresa.
- O e-mail solicita informações pessoais, como o número do cartão de crédito ou a senha de uma conta.
- O e-mail não foi solicitado e contém anexo.

13.3 Reconhecer e evitar e-mails de phishing

Phishing refere-se a tentativas fraudulentas de obter suas informações pessoais. Os golpistas usam todos os meios possíveis — e-mails e mensagens de texto falsos, anúncios pop-up enganosos, downloads falsos, spam no calendário e até mesmo chamadas falsas — para induzir você a compartilhar informações, como a senha do ID Apple ou os números dos cartões de crédito.

14- SENHAS

14.1 – O que é?

Uma **senha** ou **palavra-passe**ou ainda **palavra-chave** ou **password**, é uma palavra ou código secreto previamente convencionado entre as partes como forma de reconhecimento.

14.2- Finalidades das senhas

Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios — para agir como administradores de um sistema, por exemplo ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

MAS NÃO SÓ, como tais chaves são capazes de identificar um usuário, elas também são capazes de trazer a responsabilização cível, criminal, administrativa em caso de prática / conduta ilícita, discriminatória no mundo da web.

Enganam-se quem acredita que a internet é terra sem lei, as mesmas infrações previstas em nossas legislações também valem para o mundo digital.

15- A importância da Alteração

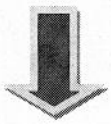
Um usuário deve alterar a senha a cada 30 dias e um histórico das 12 senhas anteriores garante que o usuário crie senhas exclusivas durante um ano.

16- Procedimentos para alterar uma senha

1- Pressionar CTRL – ALT – DEL para abrir a caixa de diálogo de login

2- Clicar no botão "changepassoword" ("alterar senha")

3- Digitar a senha atual na caixa superior



4- Digitar a nova senha onde indicado

5- Digitar a nova senha novamente para verificação.

16- A IMPORTÂNCIA DO BACKUP

Backups precisos ajudam a manter a integridade de dados, se os dados forem corrompidos. Uma empresa precisa verificar o seu processo de backup para garantir a integridade do backup, antes que ocorra perda de dados.

Aconselha-se a realização de backup periodicamente.

Entenda junto ao Departamento de TI (Tecnologia e Informação) como se dá o backup do seu Órgão.

17- DICAS PRÁTICAS

1. Como identificar um boleto falso
2. Como identificar um site de compra falso
3. Como identificar o golpe do falso financiamento:

Acesse o link e assista o vídeo abaixo:

https://g1.globo.com/fantastico/noticia/2021/01/31/mais-de-60-milhoes-de-brasileiros-ja-sofreram-com-fraude-financeira-na-internet-diz-pesquisa.ghtml

2 – Como autenticar o whatsapp em duas etapas

Acesso o link: https://www.youtube.com/watch?v=SpCONE_gYKE

Se o navegador exibir pop-ups incômodos

Se, ao navegar na Internet, você vir um pop-up ou alerta que oferece um prêmio gratuito ou que informa um problema no dispositivo, não acredite. Esses tipos de pop-up geralmente são anúncios fraudulentos, criados para induzir você a fornecer informações pessoais ou dinheiro ao golpista.

Não ligue para o número nem clique nos links para solicitar o prêmio ou corrigir o problema. Ignore a mensagem e continue navegando na página ou feche a janela ou aba.

Se uma solicitação para fazer download de software for exibida

Tenha muito cuidado ao fazer download de conteúdo da Internet. Alguns downloads disponíveis na Internet podem não conter o software que alegam ter ou podem conter software imprevisto ou indesejado. Isso inclui apps que solicitam a instalação de perfis de configuração que podem controlar seu dispositivo. Se instalados, software desconhecido ou indesejado pode se tornar invasivo e irritante e pode até danificar o Mac e roubar os dados.

Se você receber uma ligação ou voicemail suspeitos

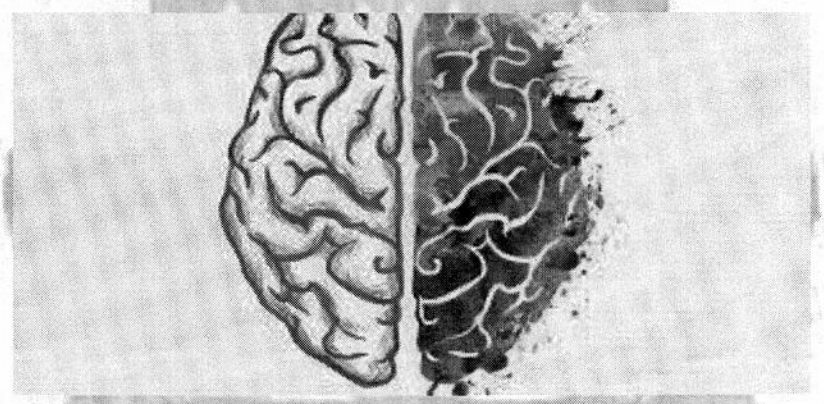
Os golpistas podem falsificar números de telefone reais de empresas e fazer elogios e ameaças como forma de pressionar você a fornecer informações, dinheiro

e até cartões de crédito. Se você receber uma ligação suspeita ou não solicitada de alguém que afirma ser da Apple, encerre a ligação.

18- MUDANÇA CULTURAL / MINDSET

MAIS IMPORTANTE: Entenda a importância dessas mudanças e coloque em prática no seu dia a dia. Será preciso mudar nossos hábitos, e isso depende da mudança em nossa mente.

COLOQUE EM PRÁTICA ESSA MUDANÇA CULTURAL!



19- CANALDE COMUNICAÇÃO

protecaodedados@aguasdaprata.sp.gov.br

Encarregada de Dados: Bruna Luísa Anadão.

©2021 | MUNICÍPIO DE ÁGUAS DA PRATA - Estância Hidromineral