Avenida Ibicuí, S/N, CEP: 97.180-000, CNPJ: 01.679.377/0001-81,
one: 55 3612 4252, http://dilermandodeaguiar.rs.leg.br, camara@dilermandodeaguair.rs.leg.br

PROJETO DE RESOLUÇÃO Nº 002/2022, DE 12 DE ABRIL DE 2022

Regulamenta a aplicação da Lei nº. 13.709/ 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), no âmbito da Câmara de Dilermando de Aguiar.

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º Esta Resolução regulamenta a aplicação da Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, adiante denominada LGPD, no âmbito da Câmara de Dilermando de Aguiar.

§ 1º Para os fins desta Lei, 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 anônimo: 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: pessoa 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 natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

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 concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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

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

XV - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVI - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVII – política de privacidade: conjunto de termos que descreve as práticas adotadas pelo site ou aplicativo em relação às informações dos usuários, tendo como função esclarecer aos usuários como os dados serão utilizados e qual finalidade.

§ 2º Esta Resolução não se aplica ao tratamento de dados pessoais realizados pelos Vereadores, quando o tratamento não utilizar sistemas oficiais da Câmara de Dilermando de Aguiar.

CAPÍTULO II
DOS PRINCIPIOS

Art. 2º As atividades de tratamento de dados pessoais deverão observar os seguintes princípios:

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

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

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

X – da 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.

CAPITULO III
DAS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Art. 3º O tratamento de dados pessoais, quando feito sem o consentimento do titular, somente poderá ser realizado com a utilização das seguintes bases legais:

I - para o cumprimento de obrigação legal ou regulatória;

II - para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

III - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

IV - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

V - para o exercício regular de direitos em processo judicial;

VI - para a proteção da vida ou da incolumidade física do titular ou de terceiros;

VII - para a tutela da saúde;

VIII - quando necessário para atender aos interesses legítimos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

IX - para a proteção do crédito.

Art. 4º A Câmara de Vereadores adotará preferencialmente o cumprimento de obrigação legal e a execução de contrato como base legal para tratamento dos dados pessoais em seus processos.

Art. 5º É dispensada a exigência do consentimento previsto no *caput* deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Resolução.

Art. 6º A Mesa Diretora como controladora quando fizer uso do consentimento como base legal e necessitar compartilhar esses dados pessoais deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Resolução.

Parágrafo Único. A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Resolução, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 7º O consentimento quando utilizado como base legal deverá ser fornecido por escrito demonstrando a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Resolução nos casos em que os dados pessoas sejam sensíveis.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, sendo as autorizações genéricas consideradas nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

§ 6º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 7º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Art. 8º O legítimo interesse, como base legal, somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador;

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Resolução.

§ 1º Quando o tratamento for baseado no legítimo interesse, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Art. 9º A Mesa Diretora da Câmara de Dilermando de Aguiar, na condição de Controladora, manterá registro das operações de tratamento de dados pessoais que realizar, especialmente quando baseado no legítimo interesse, solicitando-se, quando necessário, consentimento do titular dos dados pessoais,

observando-se que tais registros, também, deverão ser realizados por qualquer empresa contratada que atue como operadora de dados pessoais.

CAPITULO IV

DAS OPERAÇÕES DE TRATAMENTO DOS DADOS PESSOAIS

Art. 10. A operação de tratamento dos dados abrange qualquer atividade que utilize os dados pessoais, tais como:

I - acesso - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

II - armazenamento - ação ou resultado de manter ou conservar em repositório um dado;

III - arquivamento - ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;

IV - avaliação – analise do dado com o objetivo de produzir informação;

V - classificação - maneira de ordenar os dados conforme algum critério estabelecido;

VI - coleta - recolhimento de dados com finalidade específica;

VII - comunicação – transmissão da informações pertinentes a políticas de ação sobre os dados;

VIII - controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

IX - difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados;

X - distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

XI - eliminação - ato ou efeito de excluir ou destruir dado do repositório;

XII - extração - ato de copiar ou retirar dados do repositório em que se encontrava;

XIII - modificação - ato ou efeito de alteração do dado;

XIV - processamento - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

XVI - produção - criação de bens e de serviços a partir do tratamento de dados;

XVII - recepção - ato de receber os dados ao final da transmissão;

XVIII - reprodução - cópia de dado preexistente obtido por meio de qualquer processo;

XIX - transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro;

XX - transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos;

XXI - utilização - ato ou efeito do aproveitamento dos dados.

CAPITULO V

DOS DIREITOS DO TITULAR DOS DADOS PESSOAIS

Art. 11. São direitos básicos do titular de dados pessoais:

I – obter informações se a Câmara de Vereadores utiliza seus dados pessoais;

II – saber a finalidade especifica utilizada para tratamento de seus dados;

III – saber a forma e duração de tratamento de seus dados pessoais;

IV – saber quem é o controlador e como contatá-lo;

V – saber se seus dados são compartilhados e com qual finalidade;

VI – saber da necessidade de consentimento para obtenção de serviços;

VII – saber das consequências ao se negar o consentimento;

VIII – pode revogar seu consentimento de forma facilitada;

IX – poder acessar e corrigir seus dados;

X – poder solicitar o anonimato, bloqueio e eliminação de seus dados pessoais;

XI – poder realizar a portabilidade de seus dados para outros fornecedores;

XII – saber das responsabilidades dos agentes de tratamento de dados.

Art. 12. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre o atendimento do princípio do livre acesso.

Parágrafo Único. Os titulares de dados pessoais, além dos direitos previstos nesse artigo, terão assegurados os direitos de acesso a informações e respostas previstos na Lei Municipal nº. 626/2013 e na Resolução nº. 003/2013 da Casa.

CAPITULO VI

DOS TIPOS DE DADOS PARA TRATAMENTO

Art. 13. Para fins gerais de tratamento dos dados pessoas os mesmos podem ser do tipo:

I – pessoal, sendo aqueles relacionados à pessoa natural identificada ou identificável;

II – pessoal sensível, cujo tratamento pode ensejar a discriminação do seu titular;

III – anônimos que se referem a pessoas que não podem ser identificadas;

IV - dados identificados, os quais se consegue saber quem é o titular, tais como nome, identidade e CPF;

V - dados identificáveis os quais não se consegue diretamente saber quem é o titular, mas em contato com outras informações você consegue atingir seu objetivo, tais como o número do cartão de crédito, o IP do computador, nome do órgão público com o CNPJ.

Art. 14. Para fins específicos de tratamento dos dados pessoas os mesmos podem ser do tipo:

I – ideológico - tais como convicção religiosa, opiniões políticas, filiações sindicais;

II – sobre saúde – tais como informações genéticas, preservação, cuidados e recuperação;

III – sobre a vida sexual – tais como preferencias e hábitos sexuais;

IV – sobre a origem étnica – tais como costumes, crenças e tradições.

Parágrafo Único. A relação de tipos de dados pessoas não se esgota com essa relação, podendo ser ampliada conforme detalhamento da Planilha de Inventário de Dados Pessoas constante do Anexo I desta Resolução.

CAPITULO VII

DO COMPARTILHAMENTO DOS DADOS PESSOAS PELA CÂMARA DE VEREADORES

Art. 15. O compartilhamento de dados pessoais é a operação de tratamento pela qual a Câmara de Vereadores irá conferir permissão de acesso ou transferir uma base de dados pessoais a outro ente público ou entidades privadas visando ao atendimento de uma finalidade pública ou obrigação legal.

Art. 16. Em obediência a LGPD seguem os principais requisitos que devem ser observados nos processos de compartilhamento de dados pessoais pela Câmara de Vereadores de Dilermando de Aguiar:

I – a formalização e o registro;

II – o objeto e a finalidade;

III – a base legal;

IV - a forma e a duração do tratamento;

V – a transparência e os direitos dos titulares;

VI – a prevenção e a segurança.

VII – a identificação do controlador;

VIII – as informações de contato do controlador;

IX – as informações acerca do uso compartilhado de dados pelo controlador;

X – as responsabilidades dos agentes que realizarão o tratamento.

CAPITULO VIII

DA DIVULGAÇÃO DOS DADOS PESSOAIS

Art.17. A Câmara de Vereadores tem por obrigação publicar informações sobre o tratamento de dados pessoais realizados em seu sítio de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos conforme planilha de inventário constante do Anexo I desta Resolução.

Art. 18. Na divulgação dos dados a Câmara de Vereadores deve levar em conta principalmente o exercício de competências legais que permitam aos cidadãos o exercício do controle social sobre seus atos.

Art. 19. A Câmara de Vereadores desde a realização da coleta até o fim da atividade realizada com os dados pessoais, deve observar os princípios previstos nesta Resolução, verificar a base legal aplicável ao tratamento, garantir os direitos dos titulares e adotar medidas de prevenção e segurança a fim de evitar a ocorrência de incidentes com o vazamento e/ou roubo de dados.

Art. 20. Na divulgação dos dados pessoais a Câmara de Vereadores deve observar principalmente os seguintes princípios:

I - da finalidade;

II – da limitação;

III – da necessidade;

IV – da limitação de uso, retenção e divulgação.

CAPITULO IX

DO RELATÓRIO DE IMPACTO A PROTEÇÃO DOS DADOS

Art. 21. O Relatório de Impacto, documento facultativo conforme modelo constante do Anexo IV desta Resolução, irá demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas serão adotadas para mitigação dos riscos que possam afetar as liberdades e os direitos fundamentais dos titulares desses dados.

Art. 22. A elaboração contempla as seguintes etapas:

I - identificação do agentes de tratamento e do encarregado;

II – descrição do tratamento;

III – natureza do tratamento;

IV – escopo do tratamento;

V – contexto do tratamento;

VI – finalidade do tratamento;

VII – identificação das partes interessadas;

VIII – descrição das necessidades mínimas para tratamento;

IX – identificação e avaliação dos riscos;

X – adoção de medidas para tratamento dos riscos;

XI – assinatura do Presidente da Mesa Diretora e Encarregado de dados da Câmara de Vereadores.

CAPITULO X

DA SEGURANÇA DA INFORMAÇÃO RELACIONADA AOS DADOS PESSOAIS

Art. 23. A segurança da informação pode ser definida como o conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação dos titulares de dados pessoais.

Art. 24. Com relação à segurança de informação dos dados pessoais a Câmara de Vereadores deve adotar as seguintes medidas com a finalidade de promover um ambiente institucional mais seguro:

I – com a implantação de uma política de segurança da informação com o objetivo de possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação;

II – com a implantação de uma conscientização e treinamento aos Servidores e Vereadores, adotando as seguintes práticas:

a) formas de não se tornar vítimas de incidentes de segurança, tais como contaminação por vírus, que podem ocorrer ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links que chegam por e-mail;

b) não compartilhamento de logins e senhas de acesso das estações de trabalho.

III – com a implantação de um gerenciamento de contratos para atender à distribuição de funções e responsabilidades entre as partes;

IV – com a implantação de um controle de acesso com a adoção das seguintes medidas técnicas:

a) de autenticação para saber quem acessa o sistema ou os dados;

b) de autorização para saber o que o usuário identificado pode fazer;

c) de auditoria para registrar o que foi feito pelo usuário;

d) de autenticação multi-fatores (MFA) para acessar sistemas ou base de dados que contenham dados pessoais.

V – com a implantação da segurança dos dados pessoais armazenados com cópias de segurança, conhecida como backups;

VI – com a implantação da segurança das comunicações com a adoção das seguintes medidas técnicas:

a) instalação e manutenção de um sistema de firewall que monitore, detecte e bloqueie ameaças, impedindo conexões a redes não confiáveis;

b) proteção de serviços de e-mail, utilizando antivírus integrados, ferramentas anti-spam e filtros de e-mail.

VII – com a implantação de manutenções de programa de gerenciamento de vulnerabilidades com a manutenção dos sistemas e aplicativos em suas últimas versões;

VIII - com a implantação de medidas relacionada ao uso de dispositivos móveis com autenticação multi-fator para acesso aos dispositivos;

IX – com a implantação de medidas relacionadas aos serviços em nuvem com um contrato de acordo de nível de serviço que contemple a segurança dos dados armazenados.

CAPITULO XI
DA POLÍTICA DE PRIVACIDADE

Art. 25. A política de privacidade tem como finalidade esclarecer quais dados serão tratados, de que maneira e para qual finalidade.

Art. 26. Em havendo necessidade de consentimento por parte do titular dos dados pessoais por conta da base legal, a Câmara de Vereadores adotará a Política de Privacidade de Dados Pessoais conforme Anexo III dessa Resolução, correspondente à compilação de regras de boas práticas de governança para tratamento de dados pessoais, de observância obrigatória, devendo conter, no mínimo:

I – o consentimento do titular para o tratamento dos dados pessoais;

II – a relação de direitos do titular dos dados pessoais;

III – a relação de agentes que terão acesso aos dados e se esses dados serão compartilhados;

IV – a forma como os dados serão armazenados e quais medidas de segurança serão tomadas;

V – a aceitação ou não da política de cookies;

VI – os canais de atendimento;

VII – o encarregado da proteção dos dados pessoais do titular.

Art. 27. Os cidadãos Dilermandense poderão, motivadamente, solicitar adaptações à Política de Privacidade dos Dados Pessoais, conforme as respectivas especificidades, cujas propostas de adaptação elaboradas deverão ser submetidas à análise do Comitê Gestor de Governança de Dados e Informações da Câmara de Dilermando de Aguiar.

CAPÍTULO XII

DAS COMPETÊNCIAS PERMANENTES

Art. 28. Compete ao Presidente da Câmara de Vereadores como Controlador da proteção dos dados pessoais:

I - adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;

II - comunicar a ANPD e os titulares dos dados pessoais, por intermédio do Encarregado, sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

III - implementar programa de governança em privacidade, atendendo-se os requisitos mínimos do art. 50, § 2º, da LGPD, sempre que, na sua avaliação, a base legal, a estrutura, a escala e o volume das operações de tratamento de dados pessoais na sua repartição recomendarem.

Seção I

Do Encarregado De Dados Pessoais

Subseção I

Da Designação

Art. 29. O encarregado pelo tratamento de dados pessoais de que trata o inciso VIII do parágrafo primeiro do art. 1º desta Resolução, atuará como canal de comunicação entre a Câmara de Dilermando de Aguiar, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, bem como com outras entidades de proteção de dados pessoais, sendo que:

I - deve possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente conhecimentos relativos à privacidade e à proteção de dados pessoais, à análise jurídica, à gestão de riscos, à governança de dados e ao acesso à informação no setor público;

II - deve receber contínuo aperfeiçoamento relacionado aos conhecimentos de que trata o inciso I do *caput* deste artigo;

III - deve ser nomeado, por meio de portaria, no prazo de 30 (trinta) dias a contar da publicação desta Resolução;

§ 1º A identidade e as informações de contato do encarregado serão divulgadas no sítio eletrônico da Câmara de Dilermando de Aguiar, dando-se ostensiva publicidade.

§ 2º O disposto no *caput* deste artigo não impede que os demais setores da Câmara de Dilermando de Aguiar, em seus respectivos âmbitos, prestem auxílio administrativo para desempenhar os procedimentos de proteção/tratamento de dados, em interlocução com o encarregado de dados pessoais.

Art. 30. O encarregado de dados pessoais deverá receber o apoio necessário para o desempenho de suas funções, bem como ter acesso imotivado a todas as operações de tratamento de dados pessoais no âmbito da Câmara de Vereadores.

§ 1º O Encarregado pelo tratamento dos dados pessoais designado em conformidade com esta Resolução deverá desempenhar suas atribuições em articulação com o Ouvidor Geral da Câmara de Dilermando de Aguiar, não havendo impedimento para que possa ocupar as duas funções de forma conjunta.

§ 2º O Encarregado pelo tratamento dos dados pessoais deverá ser treinado e sensibilizado sobre as normas e as políticas públicas sobre proteção de dados pessoais, bem como sobre as medidas de segurança que devem ser adotadas no âmbito da Câmara de Vereadores, mediante ações de capacitação disponibilizadas.

Subseção II

Das Atribuições

Art. 31. São atividades do encarregado de dados pessoais:

I - receber reclamações e comunicação dos titulares dos dados, prestar esclarecimentos e adotar providências;

II - receber comunicações da ANPD e adotar providências;

III - orientar os Servidores e Vereadores da Câmara de Dilermando de Aguiar a respeito das práticas a serem adotadas em relação à proteção de dados pessoais;

IV - elaborar relatórios de impacto à proteção de dados pessoais, quando necessário conforme modelo constante do Anexo IV desta Resolução;

V - adotar as medidas necessárias à publicação dos relatórios de impacto à proteção de dados pessoais, na forma solicitada pela autoridade nacional;

Art. 32. Mediante requisição do encarregado de dados pessoais, os setores deverão encaminhar, no prazo assinalado, as informações eventualmente necessárias para atender solicitação da autoridade nacional ou de titulares dos direitos, devendo ser comunicadas, pelo Presidente da Casa responsável pelo tratamento dos dados:

I - a existência de qualquer tipo de tratamento de dados pessoais;

II - contratos que envolvam dados pessoais;

III - situações de conflito entre a proteção de dados pessoais, o princípio da transparência ou algum outro interesse público;

IV - qualquer outra situação que precise de análise e encaminhamento.

Art. 33. Os requerimentos do titular de dados serão direcionados ao encarregado de dados pessoais e deverão observar os prazos e procedimentos previstos na Lei Municipal de Acesso a Informação nº. 626/2013 e na Resolução nº. 003/2013.

§ 1º Os requerimentos de que trata o *caput* deste artigo serão respondidos pelo encarregado de dados pessoais com o apoio técnico da Assessoria Técnica Legislativa da Câmara de Dilermando de Aguiar.

§ 2º O pedido sobre do tratamento de dados pessoais solicitado pelo titular não se confunde com o pedido realizado com fundamento na Lei de Acesso a Informação, mantendo-se válidos os dispositivos que restringem o acesso a informações pessoais por terceiros.

Art. 34. O encarregado de dados pessoais comunicará à Mesa Diretoria da Câmara de Dilermando de Aguiar e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares informando:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Seção II
Do Operador dos Dados Pessoais

Art. 35. Compete ao operador de dados pessoais e sua equipe de apoio:

I - manter registro das operações de tratamento de dados pessoais que forem realizadas;

II - realizar o tratamento de dados segundo as instruções fornecidas pelo controlador e de acordo com as normas aplicáveis;

III - adotar, em conformidade com as instruções fornecidas pelo controlador, medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;

IV - subsidiar o controlador no intuito de dar cumprimento às solicitações, orientações e às recomendações do encarregado;

Seção III
Da Assessoria Jurídica no Tratamento dos Dados

Art. 36. Compete ao Assessor Técnico Legislativo da Câmara de Vereadores disponibilizar aos agentes de tratamento assessoria jurídica para dirimir questões e emitir pareceres do significado e alcance da LGPD e desta Resolução.

Seção IV

Do Plano de Adequação

Art. 37. O plano de adequação, como ação contínua da Mesa Diretora, deve observar, no mínimo, o seguinte:

I – a publicidade das informações relativas ao tratamento de dados, preferencialmente na página oficial da Câmara de Vereadores;

II – o 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 LGPD;

III – a manutenção de dados para o uso compartilhado com vistas à execução de políticas públicas e à disseminação e ao acesso das informações pelo público em geral;

IV – a elaboração de inventário de dados, assim entendido o registro de operações de tratamento de dados pessoais, realizados pela Câmara de Vereadores;

V - elaboração do Relatório de Impacto de Proteção de Dados Pessoais, assim entendida a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos;

VI - a adequação de contratos vigentes, conforme orientações expedidas pela Assessoria Jurídica;

VIII – a implementação da utilização de política de Privacidade conforme orientações expedidas pela Assessoria Jurídica.

CAPÍTULO XIII

DAS DISPOSIÇÕES FINAIS

Art. 38. O tratamento de dados pessoais é qualquer ação que se faça com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, devendo o seu processamento obedecer aos ditames do Manual de Regulamentação constante do Anexo II desta Resolução, elaborado pelo Comitê Gestor de Governança de Dados e Informações da Câmara de Dilermando de Aguiar e aprovado pela Mesa Diretora.

Parágrafo único. Para fins de elaboração dos demais processos de tratamento de dados pessoais no âmbito da Câmara de Dilermando de Aguiar deverão ser obedecidas as bases legais da Lei, além das diversas normas infraconstitucionais, decorrentes de tais princípios que asseguram a privacidade, a intimidade, a veracidade e o acesso dos direitos da personalidade da pessoa natural.

Art. 39. Cabe à Mesa Diretora por meio dos Setores Técnico/Administrativos/Jurídico da Câmara de Dilermando de Aguiar:

I - fornecer ao Comitê Gestor de Governança de Dados e Informações os subsídios técnicos necessários para elaboração e monitoramento de diretrizes gerais relativas às operações de tratamento de dados pessoais;

II - orientar, sob o aspecto tecnológico, a implantação da Política de Proteção de Dados Pessoais, em conformidade com as diretrizes gerais deliberadas pelo Comitê Gestor de Governança de Dados e Informações da Câmara de Dilermando de Aguiar;

III - expedir normas regulamentares necessárias ao cumprimento da LGPD após oitiva do Comitê Gestor de Governança de Dados e Informações;

IV - assegurar o cumprimento das normas relativas à proteção dos dados pessoais, de forma adequada aos objetivos da LGPD;

V - recomendar à Mesa Diretora, após oitiva do Comitê Gestor de Governança de Dados e Informações, as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto na LGPD;

VI - orientar os demais setores da Câmara de Dilermando de Aguiar no que se refere ao cumprimento do disposto na LGPD;

VI - monitorar a aplicação da LGPD no âmbito da Câmara de Dilermando de Aguiar.

Art. 40. São partes integrantes desta Resolução:

I – Planilha de Inventario de Dados constante do Anexo I;

II – Manual de regulamentação desta Resolução constante no Anexo II;

III - Política de Privacidade constante no Anexo III;

IV – Relatório de Impacto a Proteção dos Dados constante no Anexo IV.

Art. 41. Esta Resolução entra em vigor na data de sua publicação.

Dilermando de Aguiar, 12 de abril de 2022.

Ver. João Carlos Alves dos Santos
Presidente da Mesa Diretora

Ver. Marcelo Teixeira Dotto
Secretário da Mesa Diretora

Ver. Adão Escobar da Trindade
Vice Presidente da Mesa Diretora

JUSTIFICATIVA AO PROJETO DE RESOLUÇÃO Nº. 002/2022

Considerando o disposto na Lei Federal nº. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD);

Considerando que é missão da Câmara de Dilermando de Aguiar, através da Presidência, desenvolver políticas administrativas que promovam a implementação das garantias e direitos fundamentais com vistas a efetividade dos valores de justiça e de paz social;

Considerando a entrada em vigor da LGPD, bem como a crescente utilização da Internet e de modelos digitais estruturados para acesso e processamento de dados disponibilizados pelos órgãos do Poder Público;

Considerando a necessidade de elaboração de estudos e propostas voltadas à adequação no âmbito da Câmara de Dilermando de Aguiar concernente a tratamento de dados e recomendações acerca da aplicação da LGPD;

Considerando a necessidade de proteção da privacidade e dos dados pessoais dos titulares nos atos processuais e administrativos, garantia decorrente do inciso X do art. 5º da Constituição da República Federativa do Brasil,

Vem por meio dessa Resolução estabelecer as diretrizes e procedimentos que devem ser tomados pela Casa com relação a LGPD.

Como todos sabemos a LGPD estabeleceu diretrizes e normas que devem ser cumpridas por todas as instituições, públicas ou privadas, no processo de coleta, tratamento, compartilhamento, que envolvam dados dessa natureza. A intenção é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade dos cidadãos.

Sendo assim teceremos algumas considerações a respeito da implantação da Lei Geral de Proteção de Dados que devem ser analisadas por conta das dúvidas geradas no momento da implementação aqui na nossa Câmara de Vereadores e para dirimir essas dúvidas vamos elencar 13 situações a serem observadas as quais serão analisadas individualmente.

I – MANTER UMA ESTRUTURA DE GOVERNANÇA DE DADOS: Certificar de que existem pessoas responsáveis pela privacidade e gestão dos dados e procedimentos para reporte de incidentes;

II – PRESERVAR UM INVENTÁRIO DE DADOS PESSOAIS E MECANISMOS DE TRANSFERÊNCIA DE DADOS: Atestar a existência e manutenção de um inventário da localização do armazenamento de dados pessoais ou fluxo de dados, com suas classes devidamente definidas;

III – IMPLEMENTAR UMA POLÍTICA DE PRIVACIDADE DE DADOS: Redigir e executar normas relacionadas à privacidade de dados que atenda aos requisitos legais e mitigue riscos operacionais e de danos a indivíduos;

IV – INCORPORAR A PRIVACIDADE DE DADOS À SUAS OPERAÇÕES: Sustentar procedimentos operacionais consistentes com as normas internas e externas relacionadas à privacidade de dados e aos objetivos de gerenciamento de riscos;

V – CUMPRIR UM CRONOGRAMA INTERNO DE TREINAMENTO E COMUNICAÇÃO: Fornecer treinamento e comunicação contínuos para promover a conformidade com as normas internas e externas relacionadas à privacidade de dados e a mitigação de riscos operacionais;

VI – GERENCIAR OS RISCOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO: Manter um Sistema de Segurança da Informação baseado nos requisitos legais e nos riscos a que a organização está submetida;

VII – ADMINISTRAR RISCOS DE TERCEIROS: Atestar que as contratações com terceiros estão de acordo com as normas internas e externas de privacidade de dados e dentro dos limites de tolerância ao risco estabelecidos previamente;

VIII – PROVER AVISOS LEGAIS: Preparar avisos para usuários em consonância com a política de privacidade de dados, os requisitos legais e análise prévia de riscos;

IX – RESPONDER TEMPESTIVAMENTE ÀS SOLICITAÇÕES E RECLAMAÇÕES DE USUÁRIOS: Estabelecer procedimentos eficazes para interagir com os indivíduos acerca de seus dados pessoais;

X – MONITORAR NOVAS PRÁTICAS OPERACIONAIS: Observar novas práticas organizacionais para identificar eventuais novos processos ou mudanças nos processos existentes que estejam relacionados ao tratamento de dados e garantir a implementação dos princípios de Privacidade

XI – CONDUZIR DE FORMA ESTRUTURADA A APURAÇÃO E CORREÇÃO DE VIOLAÇÕES DE PRIVACIDADE: Manter um efetivo sistema de averiguação e reparação de transgressões às normas e controles e incidentes relacionados à privacidade de dados;

XII – MENSURAR A EFETIVIDADE DOS PROCESSOS E CONTROLES INTERNOS: Verificar se as práticas operacionais estão em conformidade com a política de privacidade de dados, medir e relatar a eficiência dos processos e controles internos;

XIII – ACOMPANHAR A EDIÇÃO DE NOVAS REGULAMENTAÇÕES E AS MELHORES PRÁTICAS DE MERCADO: Rastrear novos requisitos de conformidade, expectativas e as melhores práticas de mercado.

Por tais motivos, destacamos primeiramente a **necessidade de se manter uma estrutura de governança de dados**, ou seja, certificar de que existem pessoas responsáveis pela privacidade e gestão dos dados e procedimentos para reporte de incidentes.

Para tanto, sugere-se sejam seguidos os seguintes passos:

1. Nomeação de um Encarregado de Proteção de Dados responsável por supervisionar a estratégia e a implementação da proteção de dados para garantir a conformidade com os requisitos não só da LGPD, mas de outras normas internacionais as quais esteja submetida, recebendo, processando e solucionando as

reclamações e comunicações dos titulares de dados e da autoridade nacional e orientando colaboradores e terceiros a respeito das melhores práticas no que tange ao tratamento e processamento de dados pessoais. Ou seja, sua função será a de educar sobre os requisitos de conformidade, treinar todos os envolvidos, realizar auditorias regulares de segurança, manter registros abrangentes de todas as atividades e atuar como interface entre a Câmara, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

A norma não inclui uma lista de credenciais, mas recomenda-se fortemente que seja um profissional que tenha conhecimento especializado de leis e práticas de proteção de dados, que esteja alinhado com as operações, a infraestrutura e os sistemas de tecnologia da informação existentes e, principalmente, que conheça os riscos envolvidos. Idealmente, encarregado deve ter habilidades de gerenciamento e capacidade de interagir com a equipe interna, terceiros, titulares de dados e órgãos oficiais.

2. Envolver a alta administração da Câmara de Vereadores de modo que todos devem compreender os riscos cibernéticos a que está exposta, além de estarem alinhados às estratégias e objetivos das normas internas relacionadas ao processamento e tratamento de dados. Nesse sentido, recursos suficientes devem ser alocados para desenvolver, implementar, manter e melhorar os respectivos controles internos e sistemas de segurança da informação. A apresentação de reportes periódicos às partes interessadas sobre o status do processo de adequação a LGPD, neste particular, é fundamental.

3. Atribuir responsabilidades pela privacidade dos dados a todos da Câmara. A nomeação de um Encarregado de dados não o transforma no único responsável, pois é importante entender que existem departamentos que colhem e tratam dados pessoais periodicamente, tais como recursos humanos. Deste modo, os gestores devem estar amplamente envolvidos com o cumprimento da política de privacidade de dados e das obrigações legais advindas da LGPD.

4. Implementar processos de comunicação regular entre todos os envolvidos, pois uma das mudanças mais importantes que a LGPD trouxe é a obrigação de relatar em tempo razoável toda violação de dados. Procedimentos bem definidos de interação entre o Encarregado de dados e terceiros que eventualmente prestem serviços de processamento ou tratamento de dados, titulares e autoridades regulatórias devem ser sistematizados em um plano de comunicação de crise, tendo em vista o exíguo tempo para apuração e remediação de tais situações e, principalmente, os riscos reputacionais de vazamento da informação.

5. Realizar periódicas avaliações de riscos, de modo a criar uma conscientização quanto às possíveis consequências de uma violação e a importância de aprimorar os controles e sistemas de segurança cibernética, políticas e procedimentos de governança de dados. É importante verificar se as medidas técnicas e organizacionais adotadas na Câmara e por terceiros que eventualmente processem ou tratem dados para

esta, são suficientes para proteger a confidencialidade, integridade e disponibilidade dos dados. Por isso, testes de penetração regulares de sistemas de TI e de restauração do acesso a dados pessoais no caso de violações, além da revisões das melhores práticas e de novas tecnologias para mitigar o impacto de potenciais problemas, são interessantes ferramentas de auxílio ao aperfeiçoamento das estruturas de salvaguarda.

No segundo passo, vamos analisar a importância de se preservar um **inventário de dados pessoais** e definir os mecanismos de transferência de dados e assim sugere-se que as seguintes etapas sejam observadas:

1. Manter um inventário de dados pessoais e das atividades de processamento. Primeiramente, é necessário saber onde estão os dados pessoais. Para tanto, realiza-se uma auditoria na qual é identificado como são coletados e onde são armazenados os dados (se em bancos estruturados ou não-estruturados), para onde estão sendo enviados, quanto tempo são retidos e em que formatos, quem tem acesso e se está os utilizando, quem é o responsável e qual a sua relevância. Esta, certamente, será a etapa mais trabalhosa e demorada de todo o processo de adequação da organização à LGPD, pois devem ser considerados não só os servidores locais e de terceiros, mas também as nuvens públicas e privadas, mídias sociais e sites de compartilhamento, além de soluções híbridas que agregam todas as anteriores. Após este estágio, é provável que a Câmara verifique que detém dados pessoais irrelevantes, obsoletos ou redundantes, momento em que, sugere-se, sejam estes removidos de sua base, de modo a reduzir custos com o armazenamento, melhorar a indexação, dar mais rapidez ao acesso e ao tempo de recuperação na eventualidade de algum infortúnio e, sobretudo, diminuir os riscos.

2. Classificar os dados pessoais por tipo, de acordo com o seu conteúdo, preferencialmente utilizando a categorização proposta pela própria LGPD, ou seja, dado pessoal, dado pessoal sensível, e dado anonimizado. Isso ajudará a Casa a criar as políticas de armazenamento, garantir que os dados só sejam efetivamente acessados e compartilhados por pessoas com as devidas permissões e propor soluções de proteção, como criptografia contra vazamento, dando mais controle sobre as informações que circulam. Quando possível, a classificação de dados será inserida em metadados de arquivos, permitindo que essa informação trafegue com eles, informando automaticamente a aplicativos de terceiros e usuários como os dados devem ser manipulados.

No quarto capítulo, vamos discorrer acerca de como implementar uma política de privacidade de dados e, mais precisamente, como integrar este tema ao seu Programa de Integridade, redigindo e executando normas que atendam aos requisitos legais e mitiguem riscos operacionais e de danos aos titulares dos dados. Sendo assim seguem alguns passos que devem ser seguidos:

1. Elaborar ou atualizar a Política de Privacidade de Dados, utilizando linguagem simples e de fácil compreensão, evitando linguagem técnica ou jurídica, considerando seus públicos-alvo, quais sejam, os titulares dos dados.

Em resumo, a Política deve especificar:

1.1. Quais são os dados pessoais coletados pela Câmara e quais as suas finalidades;

1.2. Se são processados dados sensíveis como as informações são utilizadas;

1.3. Qual o sistema de segurança para proteção dos dados;

1.4. Quanto tempo os dados são mantidos em seu banco;

1.5. Se as informações fornecidas à Câmara são compartilhadas ou não com terceiros e, em caso positivo, quem seriam essas outras partes;

1.6. Quem é o *Encarregado*;

1.7. Quem tem acesso e quais processos utilizam-se de tais informações;

1.8. De que forma é coletado o consentimento do titular;

1.9. Como o titular pode ter acesso aos seus dados pessoais para atualiza-los ou corrigi-los;

1.10 Qual o processo para remoção dos dados de sua base ou para promover sua portabilidade;

1.11. Se os websites e aplicações da Câmara utilizam cookies;

1.12. Se é processada a transferência internacional de dados.

2. Redigir ou revisar o Código de Conduta, a Política de Segurança da Informação e outras normas internas, de modo a criar uma maior conscientização entre os Servidores acerca de questões relacionadas ao processamento e tratamento de dados e alinhar todas as normas com o mesmo discurso e as novas obrigações legais.

3. Manter um cronograma de revisão periódica dos principais documentos de integridade. Como o tema da governança de dados ainda é novo, a entrada em vigor da LGPD e a prática diária, especialmente na interação entre as partes envolvidas fatalmente trará a tona a necessidade de atualização das principais normas internas da Câmara.

Continuando com a proposta de esclarecer como a nova regulamentação influenciará nas rotinas da Câmara de Vereadores de Dilermando de Aguiar e a melhor forma de se preparar para cumprir com as novas obrigações legais, vamos exemplificar nesse quinto capitulo em que rotinas será necessário incorporar a privacidade de dados, sustentando procedimentos operacionais consistentes com as normas internas e externas e aos objetivos de gerenciamento de riscos:

1. Mapear os processos internos e aprimorar os controles de acesso. Conforme visto no capítulo anterior, deve-se revisitar ou implementar políticas e normas de conduta relacionadas à coleta, tratamento e guarda de dados pessoais, contudo a redação de documentos de nada adiantará se os processos e controles

internos não respeitarem as regras criadas internamente e as regulamentações tais como a LGPD. O mapeamento de todos os processos internos permitirá identificar com maior precisão quais são as áreas mais sensíveis da Casa e, consequentemente, onde estão os maiores riscos, no que concerne à proteção de dados, seja de clientes, usuários de sistemas de informação ou aplicações, permitindo que sejam aplicadas restrições ou implementadas melhorias nos controles de acesso a determinadas informações.

2. Integrar as normas de coleta, tratamento e guarda de dados às rotinas internas.

2.1. *No uso de cookies e mecanismos de rastreamento*. No caso dos websites de Câmara que processam dados pessoais ou que possam ser combinados ou selecionados para identificar determinada pessoa, será necessário revisar os termos de consentimento, possibilitando ao usuário de maneira ativa aceitar ou recusar os vários tipos de cookies antes de prévia configuração, informando de maneira clara por que, como e com que finalidade os dados serão utilizados e permitindo que, a qualquer momento, seja possível ter uma visão completa de todos os cookies ativos e que o consentimento possa ser revogado. Também deve restar devidamente identificado quais dados do usuário são compartilhados com terceiros em razão de aplicações que porventura estejam incorporadas ao seu website. Sob o ponto de vista das obrigações legais, deve-se registrar todos os consentimentos dos usuários, armazenando-os de forma segura para que possam ser utilizados como eventual prova.

2.2 *Na retenção de dados*. Conforme mencionado anteriormente, o inventário de dados permitirá que a Câmara livre-se de dados obsoletos, imprecisos e que eventualmente tenham sido processados sem o consentimento dos titulares evitando sua exposição às penalidades previstas pela LGPD. No entanto, com relação aos dados que permanecerão sendo processados é interessante que sejam implementados processos de categorização destes dividindo-os em categorias quanto ao tempo de retenção (curta, média ou longa, por exemplo). Importante salientar que o direito à revogação do consentimento de processamento de dados, por parte de qualquer titular, não pode se sobrepor ou contrariar outras legislações que versem sobre a obrigatoriedade de manutenção de determinados registros.

2.3. *Na contratação de terceiros e manutenção dos seus dados pessoais*. Conforme verificado anteriormente, a LGPD não diz respeito somente à garantia de conformidade para com os dados de clientes e usuários de sistemas de informação. Uma área que não deve ser menosprezada na aplicação da nova regulamentação é o de Recursos Humanos, que coleta e processa dados pessoais (efetivos e potenciais) de terceiros, seja para selecionar, contratar, demitir, pagar, fornecer benefícios, inscrever o profissional em cadastros de órgãos públicos. Neste particular, inclusive, o conceito de consentimento para tratamento e retenção dos dados se confunde com obrigações legais da Casa para execução do contrato e para cumprir com obrigações legais de ordem trabalhista e previdenciária, por exemplo, motivo pelo qual deve-se encontrar o equilíbrio entre os direitos de privacidade e a promoção de interesses legítimos da Câmara no papel de contratante. Ou seja, é fundamental que os terreiros contratados não só tenham plena consciência de suas

obrigações, como colaboradores que processam dados, mas também de seus direitos, como titulares de dados que são processados.

2.4. *Na segurança patrimonial, em especial no uso de câmeras de vigilância*. Dado pessoal é uma informação relacionada a pessoa natural identificada ou identificável, portanto vai muito além do nome, endereço, número de telefone, data de nascimento, contas bancárias, registros médicos, de modo que imagens também devem ser tratadas com o mesmo cuidado, principalmente se considerado o potencial que câmeras de vigilância conectadas à internet têm de ameaçar as liberdades individuais.

Promover uma cultura de privacidade e preservação de dados pessoais é um dos principais objetivos a serem atingidos no processo de adequação às novas regras, haja vista que sem a conscientização de todos os envolvidos é quase impossível fazer com que a Casa cumpra com todas as obrigações legais. Para tanto, sugere-se nesse sexto capitulo que seja cumprido um cronograma interno de treinamento e comunicação e a melhor forma de fazê-lo passa pelas seguintes etapas:

1. Preparar materiais com mensagens claras. Tanto no que concerne ao treinamento quanto à comunicação, é fundamental ir direto ao ponto. Deve-se certificar que a mensagem seja entendida por todos, ou seja, que cada um compreenda sua responsabilidade para com a privacidade e proteção de dados e como as novas regras impactarão suas atividades. Nesse sentido, sugere-se seja adotado um treinamento geral e breve, com um *overview* da nova regulamentação e/ou da política interna.

2. Criar um cronograma para monitorar a regularidade dos treinamentos e das comunicações. Tanto no que concerne ao treinamento quanto às comunicações, criar um plano de ação é fundamental: Para tanto, as perguntas que devem ser respondidas são as seguintes:

2.1. Que objetivos deverá ser atingido antes da entrada em vigor da nova regulamentação?";

2.2. Quais são os diferentes públicos alvos e que mensagem passar a cada um deles?";

2.3. Que meios que serão utilizados para treinar e veicular as comunicações internas?";

2.4. Em que período serão realizados os treinamentos e qual a programação das mensagens a serem veiculadas tanto ao público interno quanto ao externo?";

2.5. De quanto em quanto tempo serão realizados novos treinamentos, de modo que o discurso permaneça vivo dentro da Casa?".

3. Medir a participação e a efetividade dos treinamentos. Elaborar relatórios periódicos para determinar se os envolvidos em atividades relacionadas ao tratamento e processamento de dados participaram dos respectivos treinamentos. Sempre que possível, gerar evidências da efetividade dos treinamentos, através de questionários a serem aplicados ao término das apresentações.

4. Fornecer treinamento qualificado para o Encarregado de Proteção de Dados. Sugere-se que o encarregado participe de treinamentos específicos de educação profissional, com viés técnico e jurídico, de modo a aperfeiçoar o Programa com base nas melhores práticas de mercado.

Quando se trata da manutenção de uma estrutura de governança de dados vê-se a necessidade de realizar periódicas avaliações de riscos, visando criar uma cultura interna e aprimorar os controles e sistemas de segurança. Assim seguem algumas medidas a serem adotadas para aperfeiçoar ou sofisticar o gerenciamento dos riscos:

1. Integrar o risco de privacidade de dados em avaliações de risco de segurança. Identificar de maneira precisa todas as ameaças e vulnerabilidades relacionadas é um trabalho que está ligado à criação de um inventário de dados, ao mapeamento de acessos e de dispositivos ligados à rede de computadores. Com a identificação de *gaps* e das áreas ou dos processos mais sensíveis dentro da infraestrutura de segurança da informação será possível estabelecer uma matriz de riscos específica, considerando impacto e probabilidade das principais ameaças.

2. Manter medidas técnicas de segurança visando evitar, neutralizar ou mitigar os riscos identificados. Conforme dito anteriormente, testes de detecção e prevenção de penetração, a serem realizados regularmente nos sistemas de TI, e de restauração do acesso a dados pessoais, no caso de eventuais violações, além da adoção de salvaguardas que evitem, neutralizem ou mitiguem riscos, considerando não só a segurança cibernética, mas também a segurança física, relacionadas aos dispositivos, tudo adequado à complexidade das operações e a infraestrutura da Casa.

3. Manter medidas para criptografar dados pessoais. A criptografia é uma função que usa uma chave para codificar os dados para que apenas usuários com acesso a essa chave possam ler as informações, fornecendo proteção contra o processamento não autorizado ou ilegal de dados pessoais, contudo não pode ser usada em todo tipo de operação. Além disso, deve-se ter em mente que a própria conversão de dados pessoais de texto simples em texto cifrado representa um processamento, de modo que, ainda que criptografados, estes continuarão sendo regidos pela LGPD. Ademais, o bom gerenciamento das chaves de codificação é fundamental, do contrário o sistema de segurança não será efetivo. Recomenda-se, no caso de adoção dessa proteção, que sejam criadas diretrizes, como uma política ou procedimentos específicos, determinando que tipo de dados devem ser criptografados e/ou protegidos com uma senha.

4. Restringir o acesso a dados pessoais. O acesso aos dados pessoais, deve ser restrito àqueles com necessidade legítima. Para tanto, controles devem ser implementado, adicionando, modificando ou até mesmo excluindo perfis de usuários, garantindo ainda que o acesso seja autorizado por alguém com nível

apropriado de autoridade para autentica-los, segregando funções de modo a evitar que possam existir conflitos ou que se aumente o risco de segurança ou de privacidade.

5. Manter medidas de segurança de recursos humanos. A Câmara por possuir dados pessoais sugere-se a adoção de salvaguardas que garantam que as pessoas que acessam essas informações assinem termos de responsabilidade e confidencialidade específicos. Deve-se adotar, também, procedimentos que assegurem que quando deixam a Câmara, sejam tomadas medidas imediatas a fim de restringir o acesso a sistemas de informação e/ou instalações que abriguem dados pessoais, de modo que nenhum dado permaneça sob custódia de tais profissionais após sua transferência ou rescisão de contrato.

6. Manter uma certificação de segurança. Recomenda-se que a Câmara se submetam a auditorias específicas avaliadas por certificações de modo que se evidencie a existência e efetividade dos controles correspondentes aos sistemas de segurança da informação, proteção de dados, privacidade e governança.

Neste capítulo, o objetivo é apresentar a melhor maneira de administrar riscos de terceiro, ou seja, como atestar que os terceiros estejam alinhados com a nova regulamentação e com as normas internas de privacidade de dados, dentro dos limites de tolerância ao risco. Sendo assim podemos levar em consideração as sugeridas ações:

1. Manter requisitos de privacidade e segurança de dados em contratos firmados com terceiros (clientes, fornecedores, processadores de dados). Recomenda-se que sejam adotadas cláusulas-padrão que discorram sobre as responsabilidades na coleta, tratamento, trânsito e eliminação de dados, além de dispor sobre requisitos mínimos de segurança e confidencialidade e prever obrigações de resposta, possivelmente em um SLA (*Service Level Agreement*), no caso de eventuais violações ou vazamentos, além de especificar internamente procedimentos para executar os contratos com as partes que processam informações pessoais.

3. Realizar análise de riscos em torno da privacidade de dados. Ao selecionar fornecedores, deve-se realizar uma avaliação aprofundada da capacidade destes terceiros em cumprir com todas as obrigações legais, em especial nos casos em que há transferência de dados para servidores localizados em outros locais. As normas internas relacionadas à privacidade de dados e segurança da informação devem ser apresentadas a estes fornecedores e os controles internos também devem compreender os riscos de privacidade de dados advindos destas relações entre as partes.

3. Manter uma política para reger o uso de provedores em nuvem, de modo a garantir a regularidade e legitimidade das transferências de dados para evitar que sejam contratados ou utilizados tais serviços para armazenamento, manipulação ou troca de comunicações relacionadas à empresa sem o

conhecimento e formal aprovação do Encarregado de Proteção de Dados, que deverá certificar a segurança a privacidade e outros requisitos de tratamento. Também deve restar esclarecido na política que contas de serviços pessoais na nuvem não podem ser utilizadas para armazenamento ou transferência de dados de propriedade da empresa.

No nono capítulo vamos discorrer sobre algumas medidas para preparar avisos legais e certificar ao usuário o compromisso da Câmara para com a privacidade de dados, em consonância com as políticas, os requisitos normativos e com uma análise prévia de riscos.

Nesse sentido, alguns pontos de atenção devem ser observados:

1. Redigir avisos legais relacionados à privacidade de dados que detalhem as práticas de tratamento de dados da Casa, em linguagem clara e acessível, adaptada ao público alvo, identificando como e quais são as informações coletadas, como elas são processadas, retidas e a quem serão divulgadas ou compartilhadas, além de especificar como o titular pode acessar esses dados pessoais e solicitar a exclusão ou a portabilidade destes. Sugere-se que nos avisos legais também seja identificado quem é o Encarregado de Proteção de Dados da organização, quando esta possuir um, qual a finalidade e a base legal para processamento dos dados, se estes serão transferidos para outros países e que salvaguardas existem, e por que período os dados serão mantidos pela organização.

2. Disponibilizar os avisos legais em todas as ocasiões em que dados são coletados, seja online, em páginas da web ou e-mails, via mensagens de texto ou mesmo através de formulários físicos.

Nesta etapa, pretendo esclarecer como estabelecer procedimentos internos para responder tempestivamente às solicitações e reclamações de usuários, considerando alguns pontos fundamentais, quais sejam:

1. Desenhar um workflow para resolver eventuais reclamações de usuários ou pedidos de informação. Nesse ponto devemos manter procedimentos-padrão para:

1.1. Reconhecer reclamações relacionadas a questões de proteção de dados;

1.2. Lidar com demandas simples e relatar a resolução ao Encarregado;

1.3. Encaminhar imediatamente as demandas mais sensíveis para a Mesa Diretora pela proteção de dados.

É necessário, ainda, estabelecer e cumprir prazos para responder aos titulares de dados e mantê-los inteirados dos procedimentos para apuração ou solução das suas reclamações ou pedidos de informação, de modo a resolver as demandas a fim de se evitar que o usuário procure as autoridades competentes.

2. Manter procedimentos específicos para responder a pedidos de acesso, atualização ou correção de dados pessoais, respeitando os requisitos legais e observando os conteúdos e prazos de resposta. A resposta à solicitação de acesso, atualização ou correção de dados pressupõe dois estágios:

2.1. Primeiro verifica-se se os dados que o titular busca estão realmente sendo processados;

2.2. Em seguida, conforme disposto em lei, deve-se facilitar a consulta, informando de maneira clara a origem destes dados, a finalidade específica do seu tratamento, as categorias, os destinatários, a duração prevista do armazenamento e a identificação do controlador, com as devidas informações de contato, fornecendo os dados por meio eletrônico ou sob forma impressa no prazo previsto na lei de acesso a informações.

O grande desafio, neste particular, é entender que qualquer colaborador da organização pode receber uma solicitação válida de um titular de dados, seja aquele que tem contato direto com um cliente ou *prospect* ou aquele que monitora as redes sociais. No caso de pedidos de acesso feitos por terceiros, a organização deve estar segura de que este tem o direito de agir em nome do titular dos dados, portanto deve solicitar a apresentação de uma autorização por escrito ou procuração e em não sendo atendido este pedido sugere-se sejam divulgadas as informações diretamente ao titular. Quando os dados solicitados estiverem sendo processados por um terceiro (operador) é importante garantir que o acordo de nível de serviços preveja o cumprimento dos prazos no caso de solicitações de acesso.

3. Zelar para que processos de exclusão de dados ou portabilidade sejam respondidos correta e tempestivamente. Nos termos do Art. 18, VI, da LGPD, os titulares de dados têm direito à eliminação destes, também conhecido como “direito de ser esquecido”, quando estes não são mais necessários para o propósito para o qual foi coletado ou processado originalmente, quando o indivíduo retira seu consentimento ou quando não há interesse legítimo para continuar com o processamento. Quando a Câmara compartilhou os dados com terceiros, processadores, por exemplo, é necessário implementar um processo no qual qualquer demanda de exclusão seja notificada a estes parceiros. Importante salientar que a exclusão dos dados também deve ser realizada dos sistemas de backup, além dos sistemas ativos.

4. Conservar um chatbot de perguntas e respostas de fácil acesso pelos usuários é altamente recomendável, seja para suportar a política de privacidade e os avisos legais ou mesmo o treinamento dos Servidores.

5. Avaliar as principais causas de reclamações relacionadas à privacidade de dados, monitorando e relatando métricas. Aqui nesse ponto o Encarregado deve manter um processo para investigar as principais causas que geram reclamações de usuários e emitir recomendações para melhoria das práticas a fim de evitar queixas adicionais, gerando relatórios gerenciais para as áreas respectivas, de modo a permitir que seja medida a eficiência na resolução dos problemas e os respectivos

custos e identificando processos sensíveis, os quais acabam por expor a organização a riscos relacionados com a proteção de dados.

O presente capítulo será destinado a tratar do chamado "*Privacy by Design* ", ou seja, como identificar nas práticas operacionais novos processos, ou processos já existentes, que já estejam ou possam vir a estar relacionados à coleta, processamento e tratamento de dados, de modo a adapta-los, à nova legislação e às normas de conduta e políticas internas, visando preservar o direito à privacidade do usuário final. Assim vamos elencar alguns passos a serem seguidos:

1. Manter diretrizes e modelos detalhando como conduzir avaliações de impacto de privacidade ou avaliações de impacto de proteção de dados para garantir que os riscos de proteção de dados são medidos e analisados periodicamente quando há um novo projeto envolvendo o uso de dados pessoais, novos sistemas de segurança da informação ou o compartilhamento de dados com terceiros, e também no caso de projetos já em andamento e sistemas existentes.

2. Estruturar a avaliação de impacto de privacidade de maneira lógica e procedimentalizada. A avaliação de impacto de privacidade deve ser concebida de forma coerente, de modo a permitir que todos da casa sigam o mesmo norte quando da necessidade de realiza-la.

3. Envolver terceiros como parte destes processos de avaliações de impacto de privacidade ou de proteção de dados. Na avaliação de impacto de privacidade a participação de partes interessadas como usuários de sistemas, clientes, fornecedores e até mesmo os órgãos reguladores pode oferecer novas perspectivas sobre os riscos. Por essa razão, buscar a opinião desses *stakeholders* pode ser útil, seja por meio de *surveys* ou mesmo da imersão total para melhor entendimento de quais são e como se dará o processamento e armazenamento dos dados.

4. Acompanhar e abordar os problemas de proteção de dados identificados durante as avaliações. Uma avaliação de impacto de privacidade ou de proteção de dados geralmente é iniciada com um processo de *assessment*, na qual perguntas são feitas para identificar se a iniciativa proposta terá ou não impacto sobre os direitos e liberdades dos indivíduos quanto à proteção de dados.

5. Elaborar relatórios para os reguladores e partes interessadas, quando necessário. O relatório de avaliação de impacto de proteção de dados detalhará os riscos identificados durante o processo e os priorizará de acordo com a gravidade, devendo ainda esclarecer quais são os impactos sobre os direitos dos titulares dos dados caso os riscos venham a ocorrer, além de recomendar a adoção de controles apropriados para mitiga-los e reduzi-los a um nível aceitável. Estes relatórios poderão ser submetidos aos reguladores ou

a terceiros que tenham ou não participado do processo, para que todos sejam informados acerca dos riscos de privacidade antes do lançamento de um novo produto, sistema ou processo.

Dilermando de Aguiar, 12 de abril de 2022.

Ver. João Carlos Alves dos Santos
Presidente da Mesa Diretora

Ver. Marcelo Teixeira Dotto
Secretário da Mesa Diretora

Ver. Adão Escobar da Trindade
Vice Presidente da Mesa Diretora