sicres

Cooperativa de Crédito dos Servidores Públicos Municipais da Grande Vitória/ES

Política da Lei Geral de Proteção de Dados

Sumário

1. INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral Proteção de Dados – LGPD, com a redação dada pela Lei nº 13.853, de 8 de julho de 2019, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. OBJETIVO

O normativo tem o objetivo de preservar os dados pessoais quando do tratamento por todos os meios que seja possível a transmissão da informação relacionadas a estes dados.

Dessa forma, faz-se necessária um sentido de disciplina no que tange a proteção de dados tendo como fundamentos:

- ✓ Respeito à privacidade;
- ✓ Autodeterminação informativa;
- ✓ Liberdade de expressão, de informação, de comunicação e de opinião;
- ✓ Inviolabilidade da intimidade, da honra e da imagem;
- ✓ Desenvolvimento econômico e tecnológico e a inovação;
- ✓ Livre iniciativa, a livre concorrência e a defesa do consumidor; e
- ✓ Direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

3. APLICABILIDADE

A LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- ✓ a operação de tratamento seja realizada no território nacional;
- ✓ a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados dos indivíduos localizados no território nacional; ou
- ✓ os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

3.1. Exceções

A LGPD não se aplica ao tratamento dos dados pessoais, nas seguintes situações:

- ✓ Realizado por pessoa natural para fins exclusivamente particulares e econômicos;
- ✓ Realizado para fins exclusivamente:
  a) jornalístico e artísticos; ou
  b) acadêmicos, aplicando-se a esta hipótese os artigos 7º e 11 da Lei;
- ✓ Realizado para fins exclusivos de:
  a) segurança pública;
  b) defesa nacional;
  c) segurança do Estado; e
  d) atividades de investigação e repressão de infrações penais.

Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

4. CONCEITOS E TERMINOLOGIAS

Para que haja uma harmonização e padronização nas rotinas da SICRES compreendendo seus procedimentos internos operacionais, formalização de suas políticas, normas internas e seus contratos, faz-se necessário o conhecimento dos conceitos e terminologias, de forma que todos os envolvidos possam internalizar as

implicações envolvidas, facilitando a segregação de responsabilidades, além de desenvolver uma cultura controle tanto na equipe da SICRES, bem como nos seus parceiros e prestadores de serviços.

Nesse sentido, para fins de entendimento da LGPD considera-se;

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

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;

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

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

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

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

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

Agentes de tratamento: o controlador e o operador;

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;

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;

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

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

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

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

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;

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;

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

5. PRINCIPIOS APLICADOS AO TRATAMENTO DE DADOS

As atividades relacionadas com o tratamento de dados pessoais devem observar a boa-fé e os seguintes princípios:

Princípio 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;

Princípio da Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Princípio 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;

Princípio 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;

Princípio 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;

Princípio 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;

Princípio 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;

Princípio da Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Princípio da Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Princípios 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.

5.1. Princípios Aplicados a Segurança da Informação X Dados Pessoais

Princípio da Confidencialidade: tem-se o entendimento de que toda informação, tendo em vista o seu conteúdo e sua utilização, necessário se faz garantir sua proteção. Esta se dará limitando seu acesso e uso apenas por pessoas a quem se destina a informação, ou seja, atribui-se um grau de sigilo, que consequentemente se traduz na proteção dela;

Princípio da Integridade: considera que ao se trabalhar com informações, deve-se ter o cuidado de disponibilizá-la e mantê-la de acordo com as mesmas condições que

foi disponibilizada, protegendo a sua condição de quando foi liberada, evitando dessa forma alterações indevidas, intencional ou acidental; e

Princípio da Disponibilidade: versa sobre a informação que ao ser gerada ou adquirida por um indivíduo ou instituição, deverá encontrar-se disponível ao usuário que necessita dela para qualquer finalidade.

6. DO TRATAMENTO DE DADOS PESSOAIS

Tendo em vista o previsto na LGPD, o tratamento de dados pessoais somente poderá ser realizado observados as seguintes hipóteses:

i. mediante o fornecimento de consentimento pelo titular;
ii. para o cumprimento de obrigação legal ou regulatória pelo controlador;
iii. pela administração pública, 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, observadas as disposições do Capítulo IV desta Lei;
iv. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
v. 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;
vi. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
vii. para a proteção da vida ou da incolumidade física do titular ou de terceiro;
viii. para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
ix. quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

x. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O tratamento de dados pessoais cujo acesso seja público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Ressalta-se que para os dados tornados públicos pelo titular, resguardados os direitos do titular e os princípios previsto em Lei, a exigência do consentimento é dispensada.

No caso do Controlador que obteve o consentimento do titular e, que por necessidade de comunicação ou compartilhamento de dados pessoais com outros controladores, também deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento prevista em Lei.

Destarte que eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas na LGPD, especialmente no que concerne os princípios gerais e da garantia dos direitos do titular.

Ressalta-se que o tratamento de dados pessoais poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previsto na Lei.

6.1. Do Consentimento

Conforme previsto na Lei o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre manifestação de vontade do titular.

Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade conforme previsto na LGPD.

Ressalta-se que é vedado o tratamento de dados pessoais mediante vício de consentimento.

O consentimento deve referir-se a finalidade determinada, e as autorizações genéricas para o tratamento de dados pessoais serrão nulas.

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

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. Além disso, 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.

Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 da LGPD.

Ressalta-se que o legítimo interesse do controlador 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; e
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 da LGPD.

Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. Dessa forma, o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

6.2. Acesso Facilitado

A LGPD prevê que o titular tenha o direto ao acesso facilitado às informações sobre o tratamento de dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso, tais como:

i. finalidade específica do tratamento;
ii. forma e duração do tratamento, observados os segredos comercial e industrial;
iii. identificação do controlador;
iv. informações de contato do controlador;
v. informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
vi. responsabilidades dos agentes que realizarão o tratamento; e
vii. direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

6.3. Tratamento de Dados Sensíveis

Os dados sensíveis estão relacionados com dados pessoais sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizações de caráter religiosos, filosóficos entre outros, portanto, informações que conflitam

com os princípios que norteiam o Cooperativismo, visto que a SICRES é politicamente neutra e não faz discriminação religiosa, racial, política, filosófica e social.

Desse modo, pela sua própria natureza e complexidade dos serviços oferecidos não se faz uso de dados sensíveis nos procedimentos internos da instituição, visto que não são necessários e nem influenciam nos serviços oferecidos pela SICRES a seu quadro social.

6.4. Tratamento Dados Pessoais de Crianças e de Adolescentes

A SICRES não realiza tratativas com crianças e adolescentes, tendo que vista que seu Estatuto Social permite somente tratativas com menores entre 16 e 18 anos, desde que devidamente emancipados.

Dessa forma, considerando suas características, a SICRES não possui crianças e adolescentes que integram seu quadro social, motivo pelo qual não possui procedimentos definidos acerca do tratamento de dados para essas condições.

6.5. Término do Tratamento de Dados

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

i. verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
ii. fim do período de tratamento;
iii. comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º da Lei, resguardado o interesse público; ou
iv. determinação da autoridade nacional, quando houver violação ao disposto da Lei.

Ressalta-se que os dados pessoais serão eliminados após o término se seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

i. cumprimento de obrigação legal ou regulatória pelo controlador;
ii. estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
iii. transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei; ou
iv. uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

7. DOS DIREITOS DO TITULAR

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei. Dessa forma, o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

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 nesta Lei;
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 LGPD;
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.

O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. Além disso, 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.

Ressalta-se que os direitos do titular serão exercidos mediante requerimento expresso do próprio titular ou de representante legalmente constituído, a agente de tratamento.

Nos casos de impossibilidade de adoção imediata do requerimento, 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.

Cabe destacar que o requerimento não apresenta qualquer custo para o titular e que deve ser atendido nos prazos e nos termos previstos em regulamento. Além disso, o responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

i. em formato simplificado, imediatamente; ou

ii. por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Em caso de não oferecimento de informações baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Ressalta-se que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

8. DOS AGENTES DE TRATAMENTO DE DADOS

8.1. Do Controlador e do Operador

Tanto o controlador quanto o operador devem manter o registro das operações de tratamento de dados que realizarem, especialmente quando baseado no legítimo interesse.

O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

8.2. Do Encarregado

O controlador deverá indicar encarregado pelo tratamento de dados pessoais, bem como deverá divulgar publicamente sua identidade e as informações de contato do encarregado, de forma clara e objetiva, preferencialmente no sitio eletrônico do controlador.

As atividades do encarregado consistem em:

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 entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
iv. executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Cabe destacar que a autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

8.3. Da Responsabilidade e do Ressarcimento de Danos

A responsabilidade do controlador ou operador é extremante elevada, tendo em vista que em razão do exercício de atividades de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

A fim de assegurar a efetiva indenização ao titular dos dados:

i. o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 da Lei nº 13.709/2018; e

ii. os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 da Lei.

Na hipótese de ocorrência de processo civil por conta de dano causado ao titular, o juiz poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Nos casos de danos coletivos que tenham por objeto a responsabilização do controlador e operador, as ações de reparação podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

Cabe destacar que aquele que promover a reparação do dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Não haverá responsabilização aos agentes de tratamento de dados pessoais quando provarem:

i. que não realizaram o tratamento de dados pessoais que lhes é atribuído;
ii. que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
iii. que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Destaca-se que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

i. o modo pelo qual é realizado;
ii. o resultado e os riscos que razoavelmente dele se esperam; ou
iii. as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Além disso, responderá pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 da Lei 13.709/18, der causa ao dano.

Cabe ressaltar que nas hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

9. DA SEGURANÇA E DAS BOAS PRÁTICAS

Visando manter-se em conformidade, os agentes e tratamento devem 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.

Essas medidas devem ser observadas desde a fase de concepção do produto ou serviço até a sua execução.

Ficará a cargo da autoridade nacional a possibilidade de dispor sobre padrões técnicos mínimos para tornar aplicável as medidas de segurança, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previsto na LGPD.

Dado a necessidade de manter a segurança e o sigilo dos dados, quando houver alguma intervenção em uma das fases do tratamento, seja pelos agentes de tratamento seja por qualquer outra pessoa, estes ficam obrigados a garantir a segurança da informação em relação aos dados pessoais, mesmo após seu término.

Cabe ao controlador o dever de comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Esta comunicação deve ser realizada em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

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, observados os segredos comercial e industrial;
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.

É de competência da autoridade nacional a verificação da gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

i. ampla divulgação do fato em meios de comunicação; e
ii. medidas para reverter ou mitigar os efeitos do incidente.

No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

9.1. Das Boas Práticas e da Governança

Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular, considerando inclusive a natureza, o porte e a complexidade dos serviços e produtos oferecidos pela instituição.

9.2. Das Sanções Administrativas

Em razão das infrações cometidas às normas previstas na Lei, os agentes de

tratamento de dados, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

i. advertência, com indicação de prazo para adoção de medidas corretivas;
ii. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
iii. multa diária, observado o limite total a que se refere o inciso II;
iv. publicização da infração após devidamente apurada e confirmada a sua ocorrência;
v. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
vi. eliminação dos dados pessoais a que se refere a infração;
vii. (VETADO);
viii. (VETADO);
ix. (VETADO);
x. suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
xi. (VETADO);
xii. suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
xiii. (VETADO);
xiv. proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
xv. (VETADO);

Ressalta-se que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

i. a gravidade e a natureza das infrações e dos direitos pessoais afetados;
ii. a boa-fé do infrator;
iii. a vantagem auferida ou pretendida pelo infrator;
iv. a condição econômica do infrator;
v. a reincidência;
vi. o grau do dano;
vii. a cooperação do infrator;
viii. a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 da Lei 13.709/2018;
ix. a adoção de política de boas práticas e governança;
x. a pronta adoção de medidas corretivas; e
xi. a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

As sanções administrativas aplicadas pela autoridade nacional não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.

No cálculo do valor da multa de que trata o inciso II do artigo 52 , a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.

As sanções previstas nos incisos X, XI e XII do artigo 52 serão aplicadas:

i. somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do art. 52 deste artigo para o mesmo caso concreto;
ii. em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.

Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 da Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.

A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa O valor da sanção de multa diária aplicável às infrações a LGPD deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Ressalta-se que a intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.
42.9 DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD
Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República, cuja natureza jurídica é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. Sendo assegurada a sua autonomia técnica e decisória.

A ANPD é composta:

- Conselho Diretor, órgão máximo de direção: composto de 5 (cinco) diretores, incluindo um Diretor-Presidente;
- Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

- Corregedoria;
- Ouvidoria;
- Órgão de assessoramento jurídico próprio; e
- unidades administrativas e unidades especializadas necessárias à aplicação do disposto na Lei.

Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5.

O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor.

Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.

10. AÇÕES PARA ATENDIMENTO DA LGPD

A SICRES, tendo em vista sua natureza, seu porte e a complexidades de seu negócio e considerando que se trata de uma Cooperativa de Crédito que possui princípios congruentes com os princípios previstos na LGPD, realizou alguns ajustes com vistas a atender o previsto na Lei conforme as características da instituição identificando os pontos que necessitavam de ajustes, conforme destaque a seguir:

Ficha de Matrícula: inclusão de informações se reportando e em atendimento à LGPD, com vistas a garantir o sigilo das informações, documentos, bem como consentimento identificando a necessidade e a justificativa para o uso das informações contidas na ficha de matrícula;

Site: inclusão de informações sobre a utilização de cookies de forma a permitir que o usuário aceite ou não;

Política de Privacidade: disponibilizar a Política de Privacidade no site no link https://www.sicres.coop.br para que todos tenham acesso e conhecimento das práticas adotadas pela SICRES;

Treinamentos: realizar treinamentos e cursos para os colaboradores, conselheiros de administração e fiscal, e diretoria de forma a mantê-los atualizados sobre a LGPD;

A SICRES poderá adotar e implementar outros procedimentos internos que julgar necessário a fim de atendimento da LGPD.

11. PARÂMETROS PARA MANTER-SE EM CONFORMIDADE COM A LGPD

A SICRES para manter-se em conformidade com a LGPD deverá nortear seus procedimentos internos sempre observando os itens destacados e respeitando suas particularidades e características:

- ✓ Definição dos dados pessoais buscando assim, delimitar os direitos e as informações que serão protegidas pelo ordenamento jurídico;
- ✓ Consentimento do usuário para que haja a coleta da informação e limitação do tratamento do dado de acordo com a finalidade;
- ✓ Distinção de titularidade e responsabilidade sobre os dados, tendo em vista a necessidade de delimitação de funções e responsabilidade assumidas por conta do tratamento de dados;
- ✓ Indicação de um encarregado que ficará a cargo da comunicação entre os agentes, titulares e órgão competentes;
- ✓ Aplicação dos mecanismos pautados no livre acesso à informação e na transparência entre os usuários e as organizações;
- ✓ Aplicação de medidas de segurança e dever de reporte;
- ✓ Previsão de possibilidade de alteração e exclusão do dado pessoal;

- ✓ Aplicação de sanções no caso do descumprimento das regras; e
- ✓ Criação de órgão e/ou indicação de pessoa competente para fiscalizar e zelar pela proteção de dados pessoais e da privacidade.

12. INVESTIMENTOS PARA IMPLANTAÇÃO DA LGPD

Para atendimento da LGPD e para manter a Cooperativa em conformidade, pode haver necessidade de investimentos e este pode ser implementado em quatro níveis:

- ❖ **no nível técnico** onde são consideradas ferramentas;
- ❖ **no nível documental** onde se atualiza normas, políticas e contratos;
- ❖ **no nível procedimental** onde se considera adequação de governança e a gestão dos dados pessoais; e
- ❖ **no nível cultural** onde se realiza treinamento e campanhas de conscientização das equipes, parceiros, fornecedores e clientes.

Ressalta-se que a implementação da LGPD na SICRES, considerou o grau de complexidade da instituição, seu porte, seu grau de maturidade e aplicação de Políticas de Governanças, principalmente no que tange os dados pessoais. Além disso, será primordial a adoção de planos de respostas a incidentes, treinamentos periódicos com as equipes envolvidas e uma comunicação que ocorra de forma clara e uniforme.

13. CKECK LIST DAS AÇÕES PARA ATENDIMENTO DA LGPD

Para que a SICRES mantenha-se em conformidade com o previsto na LGPD é necessário um acompanhamento constante voltado a observância e adequação, quando aplicável, dos pontos a seguir:

- ✓ Promover a atualização da ficha cadastral dos empregados e associados;
- ✓ Promover a revisão e atualização da Política de Privacidade em consonância com o previsto nas regulamentações de proteção de dados pessoais mais recentes. Caso não haja uma política definida, necessário que seja providenciado.

- ✓ Atualizar as cláusulas contratuais que se encontre como titular de dados pessoais, tanto se consumidor final ou funcionário;
- ✓ Promover atualização das cláusulas contratuais mantidos junto aos parceiros e fornecedores, que realizam ou possuem algum acesso ao tratamento de dados. Destaque para os fornecedores de software que tratam de soluções de gestão de informação, computação em nuvem, serviço de rede e monitoração, serviços de mensageria, e-mails marketing e mídias sociais, ou seja, tudo que versar sobre coleta, produção, recepção, classificação, acesso, utilização, transmissão, armazenagem, processamento, eliminação e enriquecimento de dados;
- ✓ Verificar se o mapeamento do fluxo de dados contempla a nova definição de governança para a Tecnologia de Informação – TI, de acordo com os novos regulamentos, no que tange os controles de consentimentos considerando o ciclo de vida do dado sob a ótica da coleta, uso, compartilhamento, enriquecimento, armazenamento nacional ou internacional, com ou sem uso de nuvem, eliminação e portabilidade; e
- ✓ Prever no seu modelo de resposta de Controle de Dados, o nível de conformidade que a empresa se apresenta e se os controles são auditáveis, como forma de garantir a prevenção e aplicação de multas e fiscalizações.

14. RELATÓRIOS E DOCUMENTOS

No que tange a parte que envolve relatórios e documentos que demonstrem a aplicabilidade dos normativos na rotina das Instituições, deve-se observar:

- Atualizar o mapa que contemple o Fluxo de Dados Pessoais;
- Manter a tabela de temporalidade de guarda de dados no que versa sobre consentimento, atualizada;
- A Política de Gestão de Dados deve contemplar a assinatura inclusive de empresas do mesmo Grupo econômico, entre matriz e filial quando aplicável;
- Elaboração de Política para Tratamento de Dados Pessoais para os terceirizados que realizam tratamento de dados pessoais;
- Atualização do Termo de Uso e Política de Privacidade considerando os aspectos de tratamento, finalidade de uso, justificativa jurídica, matriz de consentimento,

novos direitos dos usuários como portabilidade, exclusão, minimização e limitação de uso;

- Atualização de cláusulas contratuais em atendimento ao previsto pela LGPD;
- Atualização de Código de Conduta considerando as cláusulas que preveem respeito à Proteção de Dados Pessoais;
- Criação de órgão competente para fiscalizar e zelar pela proteção de dados pessoais e da privacidade; e
- Por fim, atualizar a Política de Segurança da Informação considerando as cláusulas da LGPD.

Esta política entra em vigor na data de sua aprovação e vigorará por tempo indeterminado.

Conselho de Administração

MARIA JANE PEREIRA DE SOUZA PIMENTA:12542423768 Assinado de forma digital por MARIA JANE PEREIRA DE SOUZA PIMENTA:12542423768 Dados: 2022.07.15 17:35:01 -03'00'

Maria Jane Pereira de Souza Pimenta

Diretora Presidente

Assinado Certificado Digital

LINEA FRANCEZ DEPES TALLON:68913800730 Assinado de forma digital por LINEA FRANCEZ DEPES TALLON:68913800730 Dados: 2022.07.15 17:35:33 -03'00'

Linea Francez Depes Tallon

Diretora Administrativa

Assinado Certificado Digital

FERNANDO ANTONIO BARCELLOS DALVI:00974942758 Assinado de forma digital por FERNANDO ANTONIO BARCELLOS DALVI:00974942758 Dados: 2022.07.15 19:28:28 -03'00'

Fernando Antonio Barcellos Dalvi

Diretor Operacional

Assinado Certificado Digital

JOSE ANTONIO PAIVA:52634515715 Assinado de forma digital por JOSE ANTONIO PAIVA:52634515715 Dados: 2022.07.15 17:34:30 -03'00'

Jose Antônio Paiva

Conselheiro

Assinado Certificado Digital

NILZA HELENA CASTILHO FERNANDES:41689801700 Assinado de forma digital por NILZA HELENA CASTILHO FERNANDES:41689801700 Dados: 2022.07.15 17:34:04 -03'00'

Nilza Helena Fernandes Castilho

Conselheira

Assinado Certificado Digital

ANGELA MARIA BERMUDES:41650000782 Assinado de forma digital por ANGELA MARIA BERMUDES:41650000782 Dados: 2022.07.15 17:33:32 -03'00'

Angela Maria Bermudes

Conselheira

Assinado Certificado Digital

ELIAS MUGRABI DE OLIVEIRA:17155487104 Assinado de forma digital por ELIAS MUGRABI DE OLIVEIRA:17155487104 Dados: 2022.07.15 17:32:33 -03'00'

Elias Mugrabi de Oliveira

Conselheiro

Assinado Certificado Digital