Cartilha de Proteção de Dados para a Advocacia

OAB MINAS GERAIS

14ª SUBSEÇÃO
UBERABA
TRIÊNIO 2022/2024
Gestão inovadora e participativa

Comissão de Direito à Privacidade e Proteção de Dados

ÍNDICE

1 OBJETIVO DA COMISSÃO E APRESENTAÇÃO DOS COMPONENTES

A comissão tem como objetivo representar foro de discussão técnico-jurídica específico sobre a Privacidade e Proteção de Dados Pessoais, com foco profissional, legislativo, acadêmico e social; fomentar a interação e a contribuição entre profissionais, estudiosos, outras comissões, autoridades e reguladores; gerar pesquisa, conteúdo, orientações, campanhas educativas e bem como criar e/ou monitorar indicadores, propostas e sugestões para melhoria e aperfeiçoamento do tema; aproximar e fortalecer laços institucionais especialmente junto à ANPD e exercer papel de referência acerca da matéria, especialmente perante seus membros e demais advogados inscritos na OAB MG e, quando pertinente, com troca de experiências e melhores práticas em âmbito nacional e internacional.

Esta cartilha pretende ser um guia aos profissionais da advocacia, vislumbrando os novos riscos e responsabilidades advindos da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) em suas atividades profissionais. Também tem como meta auxiliar o profissional no exercício de suas atividades como consultor nos programas de adequação em proteção de dados e privacidade para organizações públicas e privadas, assim como na defesa dos interesses do cidadão titular de dados.

Dessa maneira, a leitura desta Cartilha deve ser realizada no contexto de uma relativa insegurança jurídica. Em que pese a norma e seus princípios não sofrerem alterações, é provável que a atuação judicial e a construção dessa importante disciplina pela ANPD representem fatores de mudança, para os quais devemos estar permanentemente atentos.

Esperamos com essa cartilha colaborar para o aprofundamento da cultura de proteção de dados e privacidade nas organizações e na vida quotidiana, além de

motivar os advogados para o exercício de uma de suas missões mais relevantes, a defesa dos direitos e liberdades.

A cartilha foi desenvolvida através de pesquisas feita pelo grupo que compõe a Comissão de Direito à Privacidade e Proteção de Dados.

MEMBROS DA COMISSÃO

Amanda Di-Tano | Presidente
Bruno Henrique de Oliveira Chagas | Vice-presidente
Euciely de Carvalho | 1ª Secretária
Matheus Carvalho Assumpção de Lima | 2º Secretário
Gabriella Camargo Fernandes Bicalho | 3ª Secretária
Eloá de Azevedo Caixeta | 4ª Secretária

DIRETORIA DA OAB UBERABA GESTÃO 2022-2024

Eduardo Augusto Jardim | Presidente
Rogério Carlos Santos de Pádua | Vice-Presidente
Maria Angélica Queiroz Cosci | Tesoureira
Juliana Alves Castejon | Secretária Geral
Jairo dos Santos Prata Junior | Secretário Geral Adjunto
João Paulo Borges Machado | Tesoureiro Adjunto
Israel Ferreira Candiani | Diretor Institucional

2 O QUE É LGPD?

É importante salientar que a Lei Geral de Proteção de Dados Pessoais não nasce no contexto de um vazio regulatório. Muito pelo contrário: antes mesmo de sua entrada em vigor, já havia no Brasil um amplo conjunto de legislações setoriais que regulavam, direta ou indiretamente, o tratamento de dados pessoais.

Neste contexto, é possível destacar o tratamento constitucional dado à proteção da privacidade, da intimidade, do sigilo das comunicações e à garantia do habeas data (CF, art. 5º, X, XII e LXXII). Ao lado das previsões constitucionais, há ainda uma série de legislações esparsas, aplicáveis a setores específcos. Dentre elas, é possível mencionar:

- O Código de Defesa do Consumidor (Lei nº 8.078/1990), com destaque para o seu art. 43, que dispõe sobre o direito de acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo;

- A Lei do Cadastro Positivo (Lei nº 12.414/2011), que garante uma série de direitos relacionados ao tratamento de dados pessoais para fns de análise de risco de crédito;

- A Lei de Acesso à Informação (Lei nº 12.527/2011), que traz, dentre outros elementos, uma defnição de informação pessoal, bastante semelhante, inclusive, àquela que seria consagrada pela LGPD;

- O Marco Civil da Internet (Lei nº 12.965/2014), que disciplina alguns aspectos da proteção de dados pessoais no contexto online, além de consagrar a proteção de dados pessoais como um de seus princípios gerais, dentre outras diversas normativas

Antes da promulgação da LGPD, como vimos, o que havia era um verdadeiro quebra-cabeça normativo, ou seja, diversas peças espalhadas que, muitas vezes, não se comunicavam ou não estavam em sintonia. A LGPD surge com o objetivo de harmonizar essas diferentes normativas setoriais, prevendo direitos, princípios e

garantias que pudessem servir como uma espinha dorsal a ser aplicada de forma geral e transversal a todos os setores.

Neste sentido, a LGPD harmoniza e sistematiza a regulação da proteção de dados pessoais no Brasil, reunindo as diversas legislações setoriais em torno de um núcleo e de uma lógica comuns. Assim, é possível entender a LGPD como o centro gravitacional do regime de proteção de dados pessoais no Brasil, responsável por dar sistematicidade e harmonia ao regime, devendo ser lida e interpretada em conjunto com a legislação setorial.

Ao mesmo tempo em que as regulações de proteção de dados pessoais são valiosos instrumentos de defesa e proteção de direitos e liberdades fundamentais, elas também têm amplo potencial de alavancar avanços tecnológicos, uma vez que criam novas vantagens competitivas, estimulam o desenvolvimento de soluções tecnológicas para a proteção de dados e ''obrigam'' as empresas e entidades a organizarem sua informação, o que possivelmente não ocorreria fosse outro o cenário.

Neste sentido, a tarefa de adequação à LGPD, muito antes de ser encarada como uma mera obrigação ou ônus regulatório, pode ser encarada como uma janela de oportunidades.

Um outro aspecto positivo proporcionado pelo advento da LGPD é que com ela o Brasil passa a figurar no mapa global de países que contam com leis gerais de proteção de dados pessoais. Em termos práticos, isso mostra-se extremamente relevante para que se garanta uma maior integração econômica do Brasil com outros países e blocos que já possuem suas respectivas leis gerais de proteção de dados pessoais.

3 PRINCÍPIOS APLICÁVEIS A LGPD

Princípio da Boa-Fé

A boa-fé é considerada uma premissa básica para a atividade de tratamento dos dados pessoais. Isso porque, o agente ao implementar as medidas descritas para o tratamento conforme a LGPD, por exemplo, e segui-las conforme premeditado, está agindo conforme os ditames do princípio da boa-fé.

Princípio da Finalidade

Consiste na realização do tratamento do dado pessoal para propósitos legítimos, específicos, explícitos e devidamente informados ao titular, não havendo possibilidade de tratamento posterior de forma incompatível com as finalidades inicialmente informadas. Dessa forma, o motivo da coleta deve ser compatível com o objetivo final do tratamento dos dados, uma vez que sua utilização estará sempre vinculada à motivação da coleta, sendo garantida ao titular, previamente, a informação sobre a devida finalidade da coleta.

Princípio da Adequação

Deve-se haver compatibilidade do tratamento do dado com as finalidades informadas anteriormente ao titular, de acordo com o contexto do tratamento. Por consequência, esse princípio está vinculado com ao da finalidade.

Princípio da Necessidade

O tratamento do dado deve ser limitado ao mínimo necessário para a realização de suas finalidades, mediante a avaliação de quais espécies de dados são realmente necessários, pertinentes, proporcionais e não excessivos, em relação às finalidades do tratamento de dados.

Princípio do Livre Acesso

Consiste na 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

É garantido, aos titulares, a exatidão, clareza, relevância e atualização de seus dados, de acordo com a necessidade e para cumprir com a finalidade do tratamento.

Princípio da Transparência

Consiste na 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. Nessa seara, os controladores de dados devem considerar os titulares como vulneráveis, sobretudo no meio digital, uma vez que estes possuem acesso limitado às informações disponibilizadas no ambiente cibernético.

Princípio da Segurança

Objetiva a 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

Consiste na adoção de medidas a fim de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Princípio da Não Discriminação

Versa sobre a impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

Princípio da Prestação de Contas e Responsabilização

Consiste na demonstração, por parte do agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, além de demonstrar a eficácia de tais medidas.

4 DIREITOS E DEVERES DECORRENTES DA PROTEÇÃO DE DADOS PESSOAIS

De acordo com a lei em análise, toda pessoa natural tem assegurada a titularidade de seus dados pessoais, sendo garantido a ela os direitos fundamentais de liberdade, de intimidade e de privacidade. Assim como os direitos, a lei traz, também, diversos deveres que acompanham a sistemática da proteção de dados.

TITULARIDADE DOS DADOS PESSOAIS

Em primeiro plano, cabe destacar o que é a titularidade dos dados pessoais. O titular dos dados pessoais é a pessoa física a quem se referem os dados pessoais, e o destinatário dos direitos aqui elencados. Logo, pode-se afirmar que a titularidade pertence à pessoa, que detém, por consequência, autonomia em relação ao uso dos seus dados.

O CONSENTIMENTO PARA A COLETA DE DADOS PESSOAIS

O titular é o responsável por consentir com a coleta dos seus dados, devendo ser realizada por escrito ou por outro meio que demonstre a manifestação de sua vontade. Tal consentimento pode ser revogado a qualquer momento mediante a sua manifestação expressa.

Cabe destacar, também, que em se tratando de dados sensíveis, o consentimento deverá ser específico a cada uma das informações coletadas e que existem hipóteses em que o consentimento é dispensável, em especial, quando tais dados forem indispensáveis para o cumprimento de obrigação legal ou regulatória pelo controlador, para o tratamento compartilhado de dados necessários à execução, pela administração pública, para a tutela da saúde e demais casos descritos na Lei nº 13.709/2018.

Importante salientar que a desnecessidade do consentimento não desobriga os agentes de tratamento das demais obrigações previstas na LGPD, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

DIREITO DE INFORMAÇÃO

Além de ser considerado um direito, a informação também é vista como um dever do titular de dados, pois com uma informação adequada o cidadão estará

capacitado para controlar seus dados. O fluxo dos seus dados precisa tomar forma (ser informado), sendo pressuposto para que haja qualquer tipo de processo de tomada de decisão por parte do titular dos dados. Assim, cabe ao cidadão compreender os riscos e as implicações que tal atividade trará sobre a sua esfera pessoal, a fim de racionalizar alguma decisão sobre o fluxo informacional.

O dever-direito de informação deve propiciar ao usuário os elementos necessários para o início de um processo de tomada de decisão no que tange ao fluxo de seus dados. A prestação de uma informação clara, adequada e suficiente é o portal de entrada para capacitar o cidadão com o controle dos seus dados.

DIREITO AO LIVRE ACESSO

A LGPD ao dispor a respeito do princípio da transparência, correlaciona-o diretamente à prestação de "informações claras, precisas e facilmente acessíveis", além de prever ser o consentimento nulo caso não haja esse ótimo resultado esperado: a transparência.

Assim, informação e transparência são elementos normativos unidos em virtude da tamanha correspondência entre eles, havendo um teste de eficiência do primeiro, informação, para com o segundo, transparência, como o resultado ótimo do dever-direito de informar.

Desse modo, a lei prevê o livre acesso à finalidade específica do tratamento dos dados do titular, assim como à forma e a duração do tratamento, à identificação e informações de contato do controlador, a informações sobre o uso compartilhado de dados pelo controlador e às responsabilidades das pessoas físicas e jurídicas que realizarão o tratamento, devendo tais informações serem repassadas aos titulares sem embaraço e gratuitamente.

DIREITO À SEGURANÇA DOS DADOS

A fim de garantir maior proteção à autodeterminação e preservar a segurança no tratamento de dados, medidas técnicas e administrativas deverão ser adotadas para impedir eventuais acessos não autorizados, situações ilícitas, vazamento, destruição, comunicação, difusão ou alteração de informações.

Assim, o direito à segurança dos dados está ligado, por exemplo, à adoção do processo de anonimização e outras medidas adequadas de segurança que minimizem tais riscos.

RESPONSABILIDADE DOS AGENTES DE TRATAMENTO,

Diretamente ligada ao direito à segurança dos dados pessoais, a responsabilidade dos agentes de tratamento é verificada por meio do dever que eles têm em demonstrar que adotam medidas eficazes e capazes de comprovar a observância e o cumprimento

das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Segundo a LGPD, o controlador é responsável de forma integral pelo tratamento de dados, respondendo solidariamente por quaisquer violações à legislação e/ou danos causados, tanto pelo operador quanto por outros controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular de dados.

O operador, por sua vez, responderá de forma solidária pelos danos causados quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções do controlador, hipótese em que se equipara ao controlador.

A lei ainda estabelece o direito de regresso em face aos responsáveis pelo evento danoso, exceto quando for provado pelos agentes de tratamento que não realizaram o tratamento de dados pessoais que lhes é atribuído; que, embora tenham realizado o tratamento de dados, não houve violação à LGPD; ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

DIREITO À NÃO-DISCRIMINAÇÃO

Quando se pensa em dados sensíveis, ou seja, aqueles que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação partidária, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade. Em razão disso, a LGPD entra em ação, proibindo que o tratamento de tais dados seja realizado com alguma finalidade discriminatória.

Assim, as empresas deverão tratar os dados dos titulares sem que haja qualquer tipo de discriminação ou promoção de abusos em seu desfavor. A título de exemplo, uma empresa do setor têxtil não poderá deixar de oferecer determinado produto com um valor expressivo ao consumidor, com base em sua raça, ou o local onde ele resida e, caso assim atue, estará violando o princípio da não discriminação.

DIREITO À RETIFICAÇÃO

Em consonância com a Lei do Habeas Data (Lei 9.507/1997), que é, em sua essência, a ferramenta jurídica para assegurar o conhecimento e a retificação de dados, a LGPD traz a possibilidade de o titular retificar as suas informações fornecidas, corrigindo eventuais desvios de dados e, via de consequência, de imagem e de sua personalidade. Devendo, portanto, haver o zelo pela integridade e fidelidade do conteúdo a ser divulgado a respeito do titular.

ANONIMIZAÇÃO

Dados anônimos estão fora da proteção da LGPD, uma vez que eles são relativos ao titular que não permite ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, por meio dos quais

um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Já os Dados Pseudo-Anonimizados passam por um processo semelhante ao da anonimização, exceto pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Sendo assim, o pseudo anonimato é abrangido pelo LGDP, assim como é incentivado pelo próprio regulamento como forma de reduzir os riscos.

ELIMINAÇÃO OU BLOQUEIO DOS DADOS

Bloqueio é considerado, de acordo com a LGPD, a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados. Já a eliminação, é conceituada como a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Assim como a anonimização, cabe ao titular dos dados pessoais obter do controlador, a qualquer momento, e mediante requisição o bloqueio e a eliminação dos dados desnecessários que estão sendo tratados.

Caso tenha havido o compartilhamento de tais informações, o responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados 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.

Importante ressaltar, também, que a eliminação e o bloqueio de dados é uma forma de sanção administrativa, aplicada pela autoridade nacional, quando os agentes de tratamento de dados vierem a cometer infrações às normas previstas na LGPD.

DIREITO À REVISÃO DE DECISÕES AUTOMATIZADAS

Os processos de decisões automatizados identificam um grupo, ainda que não seja possível identificar as pessoas que compõem aquela massa. Essa é uma metodologia bastante comum em muitos modelos de negócios que se valem de dados estatísticos de grupos para o direcionamento de conteúdo e publicidade. Entretanto, erros podem acontecer e o art. 20 da LGPD, garante ao titular a possibilidade de revisão de decisões automatizadas que, porventura, "afetem seus interesses".

Assim, 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.

DIREITO À PORTABILIDADE DOS DADOS

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, a portabilidade dos dados a outro fornecedor de serviço ou produto, de forma expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial, com exceção dos dados pessoais que já tenham sido anonimizados pelo controlador.

Ademais, é proibida a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos relativos à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir a portabilidade de dados quando solicitada pelo titular.

5 COMPLIANCE DE DADOS: ELEMENTOS PARA ADEQUAÇÃO À LGPD

De acordo com dados coletados pela Fundação Dom Cabral, 40% das empresas não estão preparadas integralmente para a Lei Geral de Proteção de Dados. Além disso, 86% afirmam ter conhecimento da normativa e do seu impacto. Porém, apenas 46% das organizações se reconhecem como as principais responsáveis pela implementação da LGPD dentro do seu negócio, com adequação dos processos e da política de compliance.

É essencial que os entes privados e órgãos públicos se adaptem à nova realidade e organizem seus programas de compliance, atuando com enfoque na transparência e na implementação de deveres legais exigidos para tratamento de dados pessoais, garantindo que as medidas de prevenção a incidentes sejam sempre contínuas e adotadas de forma responsável.

Assim, para haver um desenvolvimento de um ambiente de negócios em conformidade com a LGPD, diretrizes deverão ser seguidas, tais como:

1. Conhecer o titular dos dados

O primeiro ponto para adaptar à política de compliance e os processos de acordo com a LGPD é saber quem são os titulares de quem você coleta, armazena e usa os dados pessoais, podendo ser clientes, funcionários, fornecedores e entre outros.

2. Mapear os dados tratados

Nesse momento, será necessário verificar todos os dados que são tratados e utilizados pela empresa e as operações responsáveis pela sua captação, como por exemplo, marketing, vendas e RH. Tal mapeamento possibilitará a estruturação da política de privacidade, informando aos usuários sobre as finalidades dos dados coletados e explicando para que serve cada informação, o local em que elas ficarão armazenadas e o que deverá ser feito para garantir que todas as ações fiquem de acordo com a legislação.

3. Ajustar os processos de coleta e tratamento de dados

Os processos e as operações internas deverão ser adaptados para que todos os dados pessoais sejam coletados, tratados e usados de acordo com as regras, políticas de privacidade e a autorização do usuário.

4. Analisar as práticas de segurança

Um dos pontos primordiais da LGPD é a manutenção e garantia das boas práticas de segurança da informação, minimizando o risco de ataques hackers e garantindo a maior proteção dos dados pessoais. De olho neste cenário, as empresas devem analisar os mecanismos e ferramentas de cibersegurança atuais, revisá-los e atualizá-los. Assim, é possível deixar a política de compliance em conformidade com a LGPD e os melhores procedimentos de segurança.

5. Divulgar a política de compliance e facilitar o acesso

Todas as medidas acima tomadas permitem ter uma nova política de compliance totalmente adequada e atualizada, em conformidade com a LGPD. A partir daí, é possível facilitar a divulgação e disponibilização dessa política internamente.

6. Conscientizar e capacitar a equipe

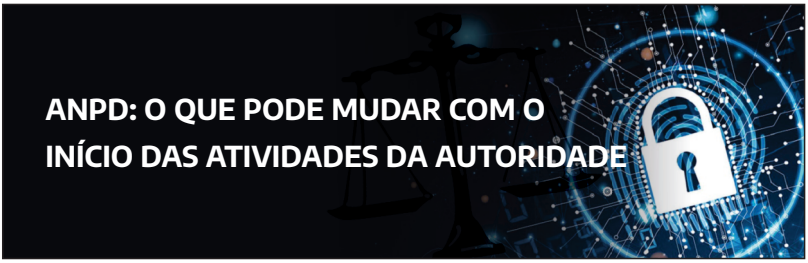
Não adianta tudo estar estruturado no âmbito de dados, operações e compliance, mas não conscientizar a equipe sobre os novos processos de conformidade. Dessa maneira, as empresas devem promover treinamentos periódicos e reciclagens para esclarecer as informações contidas na política de compliance e os ensejos sobre a LGPD.

7. Contar com um responsável por dados

Além de todo esse contexto, as organizações devem nomear um Encarregado de Proteção de Dados, também conhecido pela sigla de DPO. Este será o responsável pela gestão e monitoramento dos dados, orientação dos processos internos de segurança da informação e mediação de comunicação com os titulares e os órgãos reguladores.

Logo, este profissional será um elemento-chave dentro da política de compliance para garantir que tudo seja cumprido conforme o previsto.

6



ANPD: O QUE PODE MUDAR COM O INÍCIO DAS ATIVIDADES DA AUTORIDADE

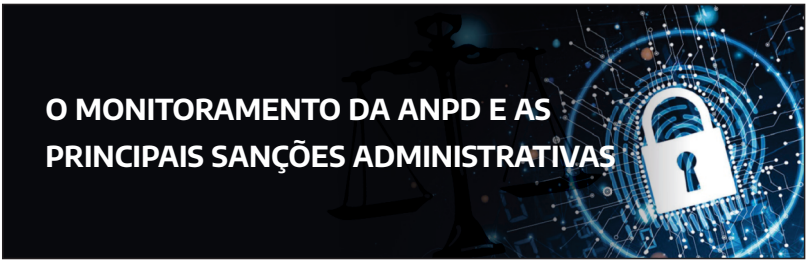
A criação da Autoridade Nacional de Proteção de Dados (ANPD) foi um passo importante e essencial para a efetiva garantia à proteção dos dados pessoais no país, bem como para a segurança jurídica das organizações públicas ou privadas.

É essencial que a ANPD possua autonomia técnica e decisória em sua atuação, para que possa assegurar a devida proteção aos dados pessoais, efetivando a segurança jurídica em sua atuação.

Com o início da atuação da ANPD no país, um dos principais pontos a serem modificados será quanto à possibilidade de aplicações de sanções administrativas, a fim de coibir o tratamento de dados em descumprimento com a LGPD, com respeito a ampla defesa e ao contraditório, além da possibilidade de interpor recurso contra a decisão proferida pela autoridade supracitada.

Com isso, com a entrada em vigor da Resolução CD/ANPD nº 1, espera-se que a seara da proteção de dados pessoais seja zelada, fiscalizada, democratizada na população, promovida perante cooperação com autoridades de até mesmo outros países, buscando, outrossim, a orientação e monitoramento, de modo preventivo e repressivo, de eventuais irregularidades na proteção de dados, por meio da Coordenação-Geral de Fiscalização.

7 O MONITORAMENTO DA ANPD E AS PRINCIPAIS SANÇÕES ADMINISTRATIVAS



O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, exercendo as competências normativas, fiscalizatórias e sancionatórias no dia 28 de outubro de 2021 aprovou a Resolução CD/ANPD nº 1, que já está em vigor, onde menciona de forma detalhada os procedimentos para aplicação de sanções administrativas e multas.

O Regulamento mencionado será aplicável às pessoas naturais ou jurídicas, que o iniciem como titulares de direitos, com interesses individuais ou no exercício do direito de representação, aqueles que, sem terem iniciado o processo, têm direitos ou interesses que possam ser afetados pela decisão a ser adotada, as organizações e associações representativas, no tocante a direitos e interesses coletivos; e as pessoas ou as associações legalmente constituídas quanto a direitos ou interesses difusos, incluindo as instituições acadêmicas, conforme mencionado no artigo 13 da Resolução.

Ainda segundo a Resolução, “a fiscalização compreende as atividades de monitoramento, orientação e atuação preventiva” da ANPD, enquanto “a aplicação de sanção ocorrerá em conformidade com a regulamentação específica, por meio de processo administrativo sancionador”

DO MONITORAMENTO

O Regulamento prevê a atividade de monitoramento da ANPD, realizada por meio da Coordenação-Geral de Fiscalização, desde que observados os limites previstos nos artigos 3º e 4º da LGPD, para, entre outras atribuições mencionadas no art. 18: (i) planejar e subsidiar a atuação fiscalizatória com informações relevantes; e (ii) considerar o risco regulatório em função do comportamento dos agentes de tratamento, de modo a alocar recursos e adotar ações compatíveis com o risco.

Como reforço a essa prática, deverá ser elaborado, anualmente, o Relatório de Ciclo de Monitoramento, que corresponde a um “instrumento de avaliação, prestação de contas e planejamento da atividade de fiscalização da ANPD”. O

primeiro Ciclo de Monitoramento terá início em janeiro de 2022. Deverá ser implementado, ainda, o Mapa de Temas Prioritários, que será bianual e "estabelecerá os temas prioritários que serão considerados pela Autoridade para fins de estudo e planejamento da atividade de fiscalização no período".

Esse último documento utilizará como critérios o risco, a gravidade, atualidade e relevância e deverá englobar: (i) a memória do processo decisório do qual decorreu a seleção e priorização dos temas, inclusive as metodologias de priorização empregadas; (ii) os objetivos a serem alcançados e os parâmetros ou indicadores usados para medir a consecução desses objetivos, quando cabível; (iii) o cronograma de sua execução; e (iv) a indicação da necessidade de interação com outros entes ou órgãos da administração pública, bem como com autoridades de proteção de dados de outros países.

DAS SANÇÕES ADMINISTRATIVAS

A LGPD previu um rol variado de sanções administrativas, de natureza admoestativa, pecuniária e restritiva de atividades. Conforme o art. 52 da LGPD, a ANPD pode aplicar as seguintes sanções administrativas:

· Advertência, com indicação de prazo para adoção de medidas corretivas;

· 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;

· Multa diária, observado o limite total a que se refere o inciso II;

· Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

· Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

· Eliminação dos dados pessoais a que se refere a infração;

· 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;

· 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;

· Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Por fim, o cálculo das multas considerará os parâmetros estabelecidos pela LGPD (art. 52). A metodologia para o cálculo ainda será submetida à consulta pública.

8 RISCOS E POLÍTICA DE PROTEÇÃO DE DADOS ESPECÍFICOS PARA ADVOCACIA

A leitura atenta e minuciosa do texto da Lei Geral de Proteção de Dados (Lei n° 13.709/18) torna inequívoca a aplicação da nova legislação aos escritórios de advocacia, nos termos do art. 5 º, inciso X, da citada lei, que disciplina que toda operação, física ou digital, realizada com dados pessoais é considerada como tratamento de dados pessoais e se submetem à adequação, incluindo, obviamente, as atividades dos escritórios de advogados.

Posto isso, como já ressaltado anteriormente, a LGPD disciplina o tratamento de dados pessoais, em meios físicos ou 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, o que certamente inclui os clientes dos escritórios de advocacia.

Com isso, os escritórios passaram, desde o ano de 2020, a ter o dever de se adaptar às imposições da LGPD, com a consequente mudança no atendimento ao cliente e no marketing, vez que todos os dados pessoais alheios precisarão ser tratados de forma a manter a conformidade com a nova legislação, além de abordar e reavaliar os processos gerenciais relativos ao tratamento de informações dos clientes, readequando os canais de relacionamento e comunicação.

Nesse rumo, mostra-se necessário que os advogados e escritórios e advocacia passem a implementar medidas de segurança quanto às informações, tanto em meio digital quanto físico, com a adoção de uma verdadeira política de proteção de dados de forma documentada, visto que as bancas também estarão sujeitas a comprovação, em caso de fiscalização pela ANPD.

Deve ser mencionado que, para que os escritórios passem a atuar em perfeita conformidade com a LGPD, também é sugerida a designação de funcionário para exercer a função de encarregado (DPO), com a realização do competente treinamento, que se responsabilizará pela interface com a Autoridade Nacional e com a comuni-

dade, no caso de solicitações referentes ao tratamento dos dados dos clientes.

Outro aspecto que deve passar a integrar a rotina dos advogados, no que concerne à LGPD, é a formulação dos contratos de prestação de serviços, que deverá informar a finalidade do tratamento dos dados pessoais dos clientes, garantindo o sigilo, em respeito, inclusive, ao próprio Código de Ética e Disciplina da OAB, que elenca o sigilo profissional com um dos deveres do advogado.

É certo também que as políticas de proteção de dados devem assegurar que todos os envolvidos na atuação estejam comprometidos com a proteção dos dados.

Diante das dicções da LGPD para os escritórios de advocacia, cumpre trazer breve resumo sobre as medidas que podem ser adotadas pelas bancas para adequação. Vejamos:

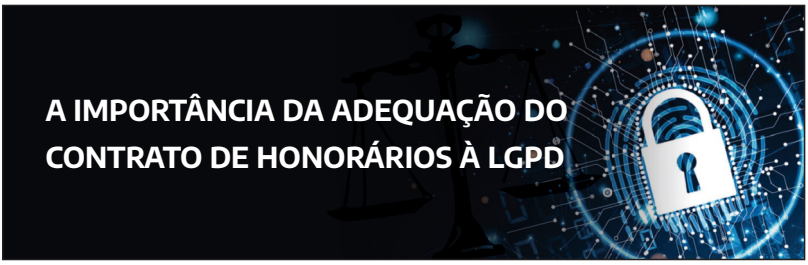
Mapeamento e registro das atividades de tratamento, sendo recomendada a elaboração de um questionário por todos os setores do escritório. Posteriormente, a realização da estruturação de Governança em Privacidade, em seguida, a elaboração da Política de Segurança da Informação e de Privacidade (por ex. bloqueio de tela de dispositivos), além da revisão dos contratos e avisos de privacidade e por fim, a conscientização dos colaboradores e dos próprios clientes.

Relativamente aos riscos decorrentes da inobservância das normas da LGPD, o que mais chama a atenção, é a possibilidade de aplicação de sanções administrativas, que variam desde a simples advertência, multa diária e multa simples de até 2% do faturamento até eliminação dos dados pessoais.

Deve ser relembrado ainda que há possibilidade de apuração da conduta do advogado por meio de processo disciplinar, por violação de sigilo, além da possibilidade de responsabilização da banca e do advogado autônomo no âmbito cível, caso seja verificado o preenchimento dos requisitos imprescindíveis, especialmente a conduta ilícita e o dano causado.

Por todo o exposto, percebe-se que existem muitos caminhos a serem trilhados pelos advogados frente à LGPD, assim como existem riscos caso não haja a observância das dicções legais.

9 A IMPORTÂNCIA DA ADEQUAÇÃO DO CONTRATO DE HONORÁRIOS À LGPD



Para que o contrato de honorários esteja em conformidade com a LGPD, é necessário que o documento contenha cláusulas de proteção de dados. O advogado possui o dever de sigilo que é inerente à profissão, no entanto, é imprescindível que o contrato em questão evidencie o compromisso com a privacidade e proteção dos dados dos clientes.

Desta forma, o contrato de honorários deverá conter, de forma expressa, cláusulas informando o seguinte que o advogado se obriga a:

- Respeitar as regras e princípios determinados pela Lei Geral de Proteção de Dados no tratamento dos dados pessoais e dados pessoais sensíveis de seus clientes. Nesta cláusula, é importante que o advogado evidencie que o contrato está alinhado ao princípio da finalidade, adequação e necessidade, que são umbilicalmente conexos, formando, juntamente com o princípio da transparência, a essência dessa norma jurídica.

- Definir a base legal que legitima o tratamento dos dados pessoais dos clientes. As bases legais estão previstas nos artigos 7º e 11 da LGPD. No entanto, tendo em vista que a contratação se deu por meio de contrato de honorários, a base legal que justifica o tratamento dos dados pessoais é a do inciso V, artigo 7º, da LGPD, qual seja: "(...) para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados."

- Informar quais são as medidas de segurança, técnicas e administrativas, utilizadas para protegerem os dados pessoais e dados pessoais sensíveis dos clientes, conforme previsão do artigo 46 da Lei Geral de Proteção de Dados;

- Informar que possui política de privacidade para clientes. É importante que o advogado tenha uma política de privacidade voltada para clientes, evidenciando a sua preocupação com o correto tratamento dos dados pessoais, inclusive sendo um diferencial de mercado.

- Informar o prazo de armazenamento dos dados, incluindo a previsão do artigo 16, da LGPD, que aduz sobre as hipóteses em que os dados pessoais poderão ser conservados mesmo após o término do seu tratamento.

10 BIBLIOGRAFIA RECOMENDADA

—ANPD Português (Brasil) (www.gov.br)

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento.Gen-Forense: Rio de Janeiro, 2019.

Como adequar a política de compliance da empresa com a LGPD. SAP Concur, 2021. Disponível em: https://www.concur.com.br/news-center/politica-de-compliance-lgpd

DONDA, Daniel. Guia Prático de Implementação da LGPD. Editora Labrador, 2020.

GARCIA, Lara Rocha. Lei GERAL DE Proteção de Dados (LGPD): Guia de Implatação. Blutcher, 2020.

GROSSI, Bernardo Menicucci (Org.). Lei Geral de Proteção de Dados: Uma Analise Preliminar da Lei 13.709/2018 e da Experiência de sua Implatação no Contexto Empresarial [Recurso Eletrônico] / Porto Alegre, RS: Editora Fi, 2020.

Lei nº 13.709/2018 (LGPD). Disponível em:
www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

MAIMONE, Flávio Henrique Caetano de Paula. Responsabilidade Civil na LGPD – Efetividade na Proteção de Dados Pessoais. Editora Foco. 2021.

Noticias - Jornal da Advocacia (oabsp.org.br)

OAB/RS - Institucional (oabrs.org.br)

RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 - RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 - DOU - Imprensa Nacional (in.gov.br)

SILVEIRA, Pedro. A LGPD comentada – Artigo por artigo da Lei Geral de Proteção de Dados. Enlaw Portal de Revistas Jurídicas. 2020.

TEPEDINO, Gustavo. Lei Geral de Proteção de Dados e Suas Repercussões no Direito Brasileiro. 2ª edição. 2020.

www.opiceblum.com.br

OAB MINAS GERAIS

14ª SUBSEÇÃO
UBERABA
TRIÊNIO 2022/2024
Gestão inovadora e participativa

Comissão de Direito à Privacidade e Proteção de Dados