Introdução a

LGPD NAS ORGANIZAÇÕES RELIGIOSAS

COMPLY LGPD

VR - VIERIA & REGINA

COMPLY LGPD

VIEIRA & REGINA

Introdução a

LGPD NAS INSTITUIÇÕES RELIGIOSAS

A LEI 13.709/2018, também chamada de Lei Geral de Proteção de Dados Pessoais, ou simplesmente LGPD, que está em vigência, parcialmente, desde agosto de 2020, veio trazer uma nova forma de instituições públicas e privadas utilizarem os dados de pessoas naturais com quem possuem relacionamento, trazendo uma série de modificações nos processos e nas formas de coleta e tratamento destes dados.

Capitulo 1

LGPD NAS ORGANIZAÇÕES RELIGIOZAS

Esta legislação não veio para proibir o uso dos dados pessoais, mas trazer padrões de condutas para serem seguidos com o objetivo de contribuir com a concretização de direitos fundamentais como a liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa, todos garantidos pela Constituição brasileira.

A Lei regula as atividades e o tratamento dos dados entre empresas, instituições de terceiro setor ou organizações religiosas, órgãos públicos e pessoas físicas. Desta forma, temos que entender o que é tratamento de dados pessoais. Pois bem, tratamento é qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados. A mera visualização de dados por um colaborador já caracteriza tratamento, estando, assim, sob o escopo da LGPD.

Na ilustração abaixo podemos ver o ciclo de vida dos dados:

Importante esclarecer que a LGPD só se aplica aos dados pessoais, que são aqueles relacionados à pessoa natural (física) identificada ou identificável.

LGPD nas organizações religiosas

Os dados pessoais identificados se referem a qualquer informação que possa individualizar seu titular, sendo relacionado a uma pessoa específica, como no seguinte exemplo:

•nome,

•sobrenome,

•endereço residencial,

•número do CPF,

•número do RG.

LGPD nas organizações religiosas

Além destes dados identificados, também é do escopo da LGPD os dados pessoais identificáveis: são aqueles que, quando analisados conjuntamente com outras características, possibilitam a identificação de uma pessoa através de referências como, por exemplo:

•profissão,
•idade,
•especialidade,
•naturalidade,
•formação,
•endereço de IP,
•geolocalização do usuário.

Existem, ainda, os dados pessoais sensíveis, que são aqueles que, devido à sua sensibilidade, podem levar a atitudes discriminatórias contra seus titulares e, por esse motivo, precisam de proteção especial. São exemplos:

•origem racial ou étnica,
•convicção religiosa,
•opinião política,
•filiação a sindicato,
•filiação a organização de caráter religioso, filosófico ou político,
•dado referente à saúde ou à vida sexual,
•imagens do sistema CFTV,
•fotos para divulgação,
•dado genético ou biométrico.

Pois bem, diante do que explicamos até momento fica a pergunta: a LGPD também se aplica às organizações religiosas? Para responder à esta questão vamos analisar o art. 4o da lei, e ver em quais situações ela não se aplica:

•quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
•para fins exclusivamente jornalístico e artísticos, ou para fins acadêmicos;
•para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;
•ou ainda em casos estrangeiros, conforme a lei.

LGPD nas organizações religiosas

Podemos, assim, observar que os templos de qualquer culto, não estão neste rol de exceções. Mas, afinal, Igreja faz algum tipo de tratamento de dados? Se a sua igreja coleta, armazena e manipula (em cadastros, meios de pagamento, ou outros registros), sim, está tratando dados para fins da LGPD! É, portanto, obrigação da igreja manter estes dados seguros e com toda a transparência que esta norma legal exige.

LGPD nas organizações religiosas

Portanto é muito importante que as igrejas se adequem à LGPD buscando mitigar os riscos relacionados ao tratamento indevido ou abusivo de dados pessoais, através da garantia de transparência e de segurança destes dados. Lembre-se: manipular dados pessoais é lidar com o direito humano fundamental de privacidade. O que está, então, em jogo, é a capacidade de agirmos com integridade na gestão eclesiástica!

Vale lembrar que em muitos casos as igrejas coletam e tratam dados pessoais, desde a simples visita de pessoas que não congregam naquela organização religiosa, para um futuro contato, passando pelos dados necessários para o controle dos membros, além das fotos e/ou filmagens registradas nos cultos e que, muitas vezes vão parar no site ou outras formas de divulgação. Site este que também deverá ser adequado às regras impostas pela LGPD.

Além destes exemplos mais simples, comumente temos também informações financeiras, atas e correspondências, dados de crianças e adolescentes, pedidos de oração etc. Para todos estes casos temos que garantir a transparência no uso destes dados, bem como a segurança dos mesmos, esclarecendo aos titulares a finalidade relacionada ao dado que está sendo coletado, as formas de utilização deles, bem como a retenção e descarte, sendo necessário manter o registro sobre o tratamento dos dados.

Aqui está a chave: o tratamento correto e organizado dos dados pessoais é uma medida de compliance: de cumprimento, adequação, respeito no trato de informações sensíveis de outras pessoas. Isto fala muito no ambiente religioso, aonde a ética vem antes mesmo da lei! Esta mudança cultural será primordial nos tempos da convivência digital que estamos experimentando, especialmente durante e após a pandemia do novo corona vírus.

Sua igreja está preparada para servir na era da democracia digital?

Capitulo 2

O QUE DEVO SABER PARA FAZER A ADEQUAÇÃO À LGPD?

Primeiramente temos que entender alguns conceitos e princípios dessa lei, para que possamos saber por onde começar. A LGPD nos traz uma estrutura de governança que apresenta algumas figuras definidas que vamos apresentar aqui. Na imagem abaixo, temos uma estrutura gráfica que ilustra melhor os principais envolvidos nesta legislação.

O QUE DEVO SABER PARA FAZER A ADEQUAÇÃO À LGPD?

A seguir, descrevemos melhor cada um destes elementos:

TITULAR DOS DADOS: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento nos processos da organização, pelo fato de que, de alguma forma estão relacionadas com as atividades legítimas. Como exemplos, nas igrejas, temos os membros, os empregados, os obreiros, ou qualquer outro em que seja necessário o tratamento de dados pessoais.

CONTROLADOR: No âmbito interno, o controlador é o representante legal da igreja, normalmente o pastor titular, que é o responsável por ela, que por meio dos seus poderes e atribuições delega as ações necessárias para operacionalizar a Política da Proteção de Dados Pessoais e Privacidade dentro da estrutura. Para o ambiente externo, o Controlador é a própria igreja que exigirá das pessoas físicas e das pessoas jurídicas, de Direito Público ou Privado, com quem se relaciona, o cumprimento dessa política quando aquelas estiverem tratando dados pessoais originários da Organização.

O QUE DEVO SABER PARA AÇÃO À LGPD? O QUE DEVO FAZER A ADEQUAÇÃO

ENCARREGADO DE DADOS: Pessoa natural, indicado pelo controlador, cujas atribuições estão definidas nos incisos do Parágrafo 2o do Art. 41 da LGPD que são:
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; e
IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
Todas as igrejas precisarão de um DPO, porém, este pode ser terceirizado, o que reduz custos e garante a independência e conhecimento necessários ao mesmo.

OPERADORES INTERNOS: São todos os colaboradores ou obreiros que, na execução das atividades relativas aos processos da igreja, têm contato e tratam dados de pessoas naturais.

OPERADORES EXTERNOS: São as organizações que compõe o Ecossistema da Proteção de Dados da Organização que, para cumprir legislações e atividades específicas relacionadas com as finalidades da igreja, tratam dados dos titulares a ela vinculados. Por exemplo, um escritório que preste serviços jurídicos ou contábeis para a igreja, e acessam dados pessoais controlados por ela, são operadores externos.

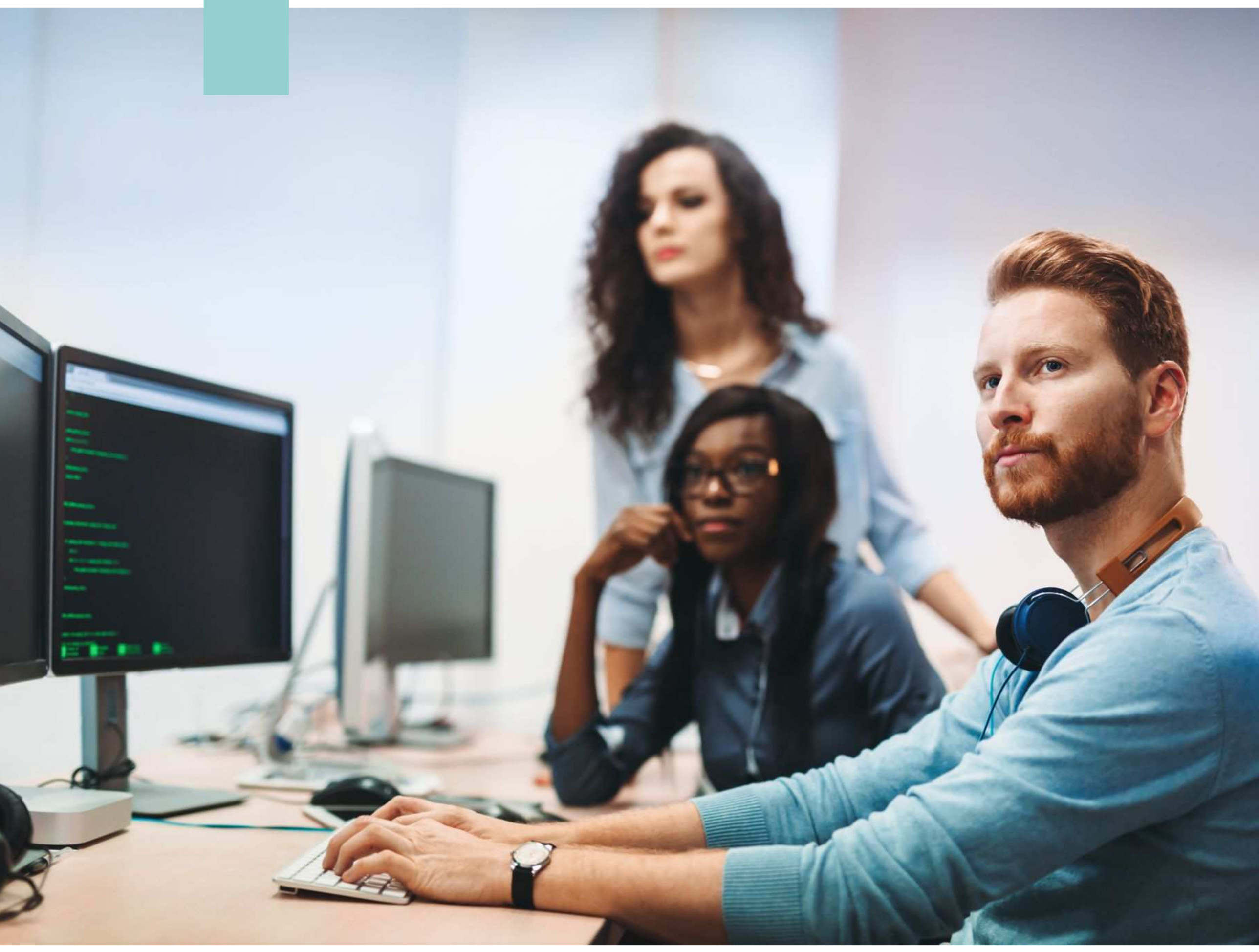
ANPD: Autoridade Nacional de Proteção de Dados (ANPD) – Órgão da administração pública que é responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

PRINCÍPIOS DA LGPD

1. **FINALIDADE**
   Tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.
2. **ADEQUAÇÃO**
   Compatibilidade do tratamento com as finalidades informadas ao titular.
3. **NECESSIDADE**
   Limitação do tratamento ao mínimo necessário para a realização de suas finalidades.
4. **LIVRE ACESSO**
   Consulta facilitada e gratuita sobre a forma e a duração do tratamento.
5. **QUALIDADE DOS DADOS**
   Garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento.
6. **TRANSPARÊNCIA**
   Garantia de informações claras, precisas e facilmente acessíveis sobre o tratamento dos dados.
7. **SEGURANÇA**
   Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais.
8. **PREVENÇÃO**
   Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
9. **NÃO DISCRIMINAÇÃO**
   Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
10. **RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS**
    Demonstração, pelo agente, da adoção de medidas eficazes.

Capitulo 3

BASES PARA COLETA E TRATAMENTO DE DADOS



A LGPD autoriza, em seu art. 23, empresas e organizações em geral a realizar o tratamento de dados pessoais unicamente para o atendimento de sua finalidade específica, com o objetivo de executar as competências legais ou cumprir as atribuições contratualmente ajustadas, desde que as hipóteses de tratamento sejam informadas ao titular.

O tratamento de dados pessoais poderá ser realizado, portanto, desde que esteja enquadrado em uma das hipóteses elencadas no art. 7o. Tais hipóteses devem ser compreendidas como condições necessárias para verificar se o tratamento de dados a ser realizado pelo controlador ou operador é permitido.

Aqui podemos ver quais são estas bases legais que legitimam o tratamento de dados conforme a LGPD:

BASES PARA COLETA E TRATAMENTO DE DADOS

CONSENTIMENTO: o consentimento fornecido pelo titular é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5, XII, LGPD). A rigor, a necessidade do consentimento concretiza a autonomia da vontade do usuário. Temos que ter o cuidado que, ao utilizar esta base legal, podemos perder esta possibilidade de tratar estes dados, considerando que um dos direitos do titular é revogar o consentimento a qualquer tempo. Importante observar que, mesmo com o consentimento do titular, os dados não passam a pertencer à igreja, ou seja, eles são sempre de propriedade dos titulares.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA: esta base legal é uma regra de legalidade ampla que busca preservar o interesse público. Em resumo, esta hipótese de tratamento de dados se concretiza por força de lei anterior ou para garantir a ordem e segurança social, tendo como fundamento garantir a segurança jurídica

EXECUÇÃO DE POLÍTICAS PÚBLICAS: a administração pública, poderá fazer o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou previstas em contratos, convênios ou similares, observadas as disposições do Capítulo IV da LGPD.

ESTUDO POR ÓRGÃOS DE PESQUISA: Com relação à realização de estudos e de pesquisas, essa hipótese de tratamento de dados é válida para as entidades públicas e privadas. Neste caso, prevalece o interesse público diante dos resultados dos estudos e pesquisas.

EXECUÇÃO DE CONTRATO: partindo-se da premissa de que o contrato legaliza a relação entre as partes, uma vez celebrado deverá ser cumprido na sua integralidade, nas condições em que prevalece a autonomia da vontade. Ou seja, em havendo necessidade de tratamento de dados pessoais com o objetivo de cumprimento ou realização dos termos ajustados em contrato, o consentimento do titular pode ser inferido pela expressão de vontade no momento da formalização do contrato.

EXERCÍCIO REGULAR DE DIREITO: para esta base legal, o tratamento de dados pode ser feito 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). A base legal do exercício regular de direitos esclarece que a proteção aos dados pessoais não compromete o direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais da parte concorrente.

BASES PARA COLETA E TRATAMENTO DE DADOS

PROTEÇÃO DA VIDA: o tratamento de dados pode ser autorizado quando for indispensável à proteção da vida ou à segurança física do titular ou de terceiro, ainda que sem o consentimento do titular.

TUTELA DA SAÚDE: esta base legal se presta exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, sendo a única que relaciona o direito a um agente exclusivo.

PROTEÇÃO AO CRÉDITO: essa base legal de tratamento serve como garantia ao controlador no recebimento de seu crédito, além de possibilitar a análise de crédito pelas organizações.

LEGÍTIMO INTERESSE: uma das bases mais propagadas, o tratamento com base no legítimo interesse autoriza o controlador a tratar dados pessoais para diversas finalidades, desde que consideradas legítimas, tais como (i) apoio e promoção de atividades do controlador e (ii) prestação de serviços que beneficiem o titular de dados, desde que respeitados os direitos e liberdades fundamentais do titular, que exijam a proteção de seus dados. Neste caso, se faz necessário justificar o interesse legítimo e, uma das formas é através do balanceamento do interesse legítimo. Esta hipótese significa a vontade do controlador, ou da sociedade, em se beneficiar de forma legal com o tratamento de dados pessoais, desde que as legítimas expectativas do titular sejam respeitadas.

Capitulo 4

DIREITOS DOS TITULARES DE DADOS

Além de regulamentar as diretrizes que as empresas devem seguir ao lidar com dados pessoais, a Lei Geral de Proteção de Dados também assegura os direitos dos titulares de dados. Para um processo de adequação à lei, é fundamental conhecer o que, exatamente, a LGPD elenca como sendo esses direitos, que estão expressos no Art. 18 da lei.

Ainda, a LGPD deixa claro, em seu Art. 17 que os dados pertencem ao indivíduo, e não à empresa/ instituição que controla ou opera esses dados.

> "Art. 17. 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 desta Lei."

Sendo assim, ficam expressos os direitos do titular de dados, conforme seguem:

DIREITOS DOS TITULARES DE DADOS

1.Confirmação da existência de tratamento: segundo a LGPD, o titular dos dados tem o direito de confirmar se uma empresa realiza o tratamento de seus dados pessoais. A LGPD estabelece ainda que a resposta pode ser feita de forma imediata e de maneira simplificada, ou por meio de declaração “clara e completa”, que indique a origem dos dados, os critérios usados e a finalidade do tratamento. O prazo para a resposta no formato completo é de até 15 dias contado a partir da data do requerimento, conforme estabelece o Art. 19.

2.Acesso aos dados: além de saber se a empresa trata seus dados pessoais, o titular também pode pedir acesso aos dados. Ou seja, é possível obter uma cópia dos dados pessoais que a empresa possui em seus arquivos.

3.Correção de dados: outro direito do titular de dados é solicitar à empresa a correção de dados pessoais incompletos, inexatos ou desatualizados.

4.Anonimização, bloqueio ou eliminação de dados: caso queira, o titular de dados também tem o direito de solicitar a anonimização (processo que torna um dado impossível de ser vinculado a um indivíduo), bloqueio ou eliminação de dados quando eles forem “desnecessários, excessivos ou tratados em desconformidade” com a lei. Por exemplo, se a empresa trata dados que não são necessários para alcançar a finalidade do tratamento ou se o tratamento não é enquadrado em nenhuma das bases legais previstas na lei.

5.Portabilidade dos dados: por este direito o titular de dados pode solicitar a portabilidade dos dados, ou seja, a transferência das suas informações pessoais a outro fornecedor de serviço ou produto.

6.Eliminação dos dados tratados com consentimento: nos casos em que o titular dos dados consentiu com o tratamento, mas mudou de ideia e não quer mais que a empresa trate seus dados pessoais, ele pode solicitar a eliminação desses dados. No entanto, há situações em que esse direito não pode ser exercido, como quando a empresa precisa conservar os dados para cumprir obrigação legal ou regulatória.

7.Informações sobre o compartilhamento de dados: considerando que um dos princípios da LGPD é a transparência, é direito do titular saber exatamente com quem o controlador está compartilhando seus dados.

8.Informação sobre a possibilidade de não fornecer consentimento: a premissa do consentimento é que ele seja pedido e concedido de forma clara, transparente e totalmente livre. Para isso, o titular de dados tem o direito de ser informado sobre a possibilidade de não fornecer o consentimento e de quais as consequências caso o consentimento seja negado.

9.Revogação do consentimento: segundo apregoa a LGPD, qualquer consentimento dado para o tratamento de dados pessoais pode ser revogado. Este é um direito do titular de dados, que pode fazer uma solicitação revogando o consentimento, o que é diferente da eliminação de dados, tratada anteriormente.

Capitulo 5

SEGURANÇA DA INFORMAÇÃO

Como já visto nas considerações anteriores, a LGPD tem dois pilares fundamentais, quais sejam: transparência e segurança. Até agora, falamos muito na transparência e como devemos garanti-la. Vamos falar um pouco sobre segurança.

Conforme consta na exposição de motivos da LGPD, um dos fatores que motivou sua promulgação foi o avanço da tecnologia da informação e a exacerbada quantidade de dados pessoais expostos na Internet, motivando o legislador a empreender esforços para conferir maior proteção às informações dos cidadãos e à sua privacidade.

Nesse sentido, a LGPD introduz novas responsabilidades e práticas que devem ser observadas e cumpridas por todos aqueles que realizam tratamento de dados pessoais, dedicando o capítulo VII da lei às medidas de segurança e boas práticas que devem ser adotadas para garantir e a segurança e a proteção dos dados.

SEGURANÇA DA INFORMAÇÃO

A segurança da informação está diretamente relacionada com a proteção de um conjunto de informações, a fim de preservar o valor que possuem para um indivíduo ou uma organização. A segurança da informação tem por propriedades básicas: a confidencialidade, a integridade, a disponibilidade e a autenticidade, propriedades essas que passo a explicar:

• Confidencialidade: grau em que o acesso à informação é restrito a um grupo definido e autorizado a ter esse acesso. A confidencialidade é um princípio da segurança da informação que garante que os arquivos da empresa sejam acessados somente por pessoas autorizadas, controlando e restringindo acessos;

• Integridade: refere-se à manutenção das condições iniciais das informações de acordo com a forma em que foram produzidas e armazenadas. A integridade é o princípio da segurança da informação que garante que os dados estejam em sua originalidade e não alterados ou corrompidos.

• Disponibilidade: grau em que as informações estão disponíveis para o usuário e para o sistema de informações que está em operação no momento em que a organização exige. É o princípio da segurança da informação que garante que os dados possam ser acessados sempre que necessário.

• Autenticidade: propriedade que algo/ alguém é o que diz ser. É o processo de identificar e registrar o usuário que está enviando ou modificando uma informação.

Para garantir que esse cenário de segurança da informação se concretize e por entender que as organizações são responsáveis por manter a segurança e sigilo dos dados pessoais sob sua responsabilidade, a LGPD estabelece, de maneira bastante objetiva, em seus artigos 46 a 49, que os agentes de tratamento de dados (o Controlador e o Operador Externo) devem lançar mão de todas as medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais tratados contra acessos não auto- rizados ou outras situações ilícitas

Capitulo 6

POR QUE DEVEMOS NOS ADEQUAR À LGPD?

São vários os impactos para quem não cumprir com a LGPD, e devem ser divididos em duas instâncias, a judicial e a administrativa. Na judicial, os titulares de dados, desde o início da vigência da lei, já podem judicializar as situações de descumprimento, sendo que, já temos pequenas, médias e grandes empresas condenadas. A indústria das ações indenizatórias com base na LGPD já iniciou.

Quanto à esfera administrativa, esta foi adiada para 1o de agosto de 2021, em função da lei 14.010/2020, que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Esta lei determinou, em seu artigo 20 que os artigos 52, 53 e 54 da lei 13709/2018 seriam postergados para o dia 1o de agosto de 2021.

POR QUE DEVEMOS NOS ADEQUAR À LGPD?

A Autoridade Nacional de Proteção de Dados (ANPD), conforme já falamos, é o grau hierárquico máximo da Lei Geral de Proteção de Dados. A ANPD será responsável por fiscalizar o tratamento de dados em todo o território nacional e aplicar as correções e sanções pertinentes, caso a lei seja desobedecida.

São várias as penalidades que podem ser aplicadas pela ANPD. Discriminadas no artigo 52 da LGPD, elas variam entre aplicação de advertências, com indicação de prazo para adoção de medidas corretivas, multas, ou até mesmo a proibição total ou parcial de atividades relacionadas ao tratamento de dados. As multas, por sua vez, vão de 2% (dois por cento) do faturamento da empresa no último exercício com teto máximo de R$ 50.000.000,00 (cinquenta milhões de reais) por infração, existindo, ainda, a possibilidade de incidência de multa diária para compelir a entidade a cessar as violações. De toda forma, a aplicação de qualquer dessas penalidades pode ter impacto bastante negativo sobre a atividade empresarial, não somente no aspecto financeiro, mas também no reputacional e operacional.

Para a correta mensuração e aplicação das sanções, ANPD deverá considerar os seguintes parâmetros:

•A gravidade e a natureza das infrações e dos direitos pessoais afetados;
•A existência de mecanismos internos de correção e proteção de dados;
•A pronta adoção de medidas correti- vas;
•Boa-fé;
•A extensão do dano causado;
•A condição econômica do infrator
•A adoção de política de boas práticas e governança em proteção de dados
•A reincidência
•A proporcionalidade entre a gravidade da falta e a intensidade da sanção
•A cooperação do infrator
•A vantagem auferida ou pretendida pelo infrator.

Capitulo 7

O QUE DEVEMOS FAZER PARA GARANTIR UMA BOA ADEQUAÇÃO?

Para que a organização se adeque à LGPD é necessário fazer um bom projeto de implementação, devendo seguir os seguintes passos:

QUE DEVEMOS FAZER PARA GARANTIR UMA BOA ADEQUAÇÃO?

1. Analisar de que Forma a organização é impactada pela LGPD:

(i) Como, por que, e quais categorias de dados pessoais são tratadas pela organização;
(ii) Analisar o ciclo de tratamento de dados pessoais, desde a coleta até o descarte, identificando a finalidade da utilização.

2. Analisar e documentar as bases legais para o tratamento de dados, para aqueles submetidos à LGPD.

3. Obter os consentimentos necessários, se for o caso.

4. Revisar e detalhar a politica de privacidade, tornando públicos os seus termos aos interessados.

5. Definir e documentar as bases legais das transferências internacionais de dados, se for o caso.

6. Adaptar os canais de comunicação e a politica e os processos internos destinados a atender os direitos dos titulares.

7. Designar o encarregado de proteção de dados.

8. Revisar os acordos e contratos da organização impactados pela LGPD.

9. Desenhar e implementar as medidas necessárias para garantir a segurança dos dados.

10. Implementar políticas e procedimentos para lidar com a ocorrência de eventuais incidentes.

11. Identificar os possíveis riscos no tratamento de dados, de modo que as medidas necessárias para reduzi-los sejam indentificadas e implementadas.

DICAS PARA REALIZAR UMA BOA ADEQUAÇÃO

Em que pese estejamos sujeitos a imaginar que, por ser uma lei, a implementação deverá ser feita por um advogado ou escritório jurídico, os requisitos da LGPD estão muito mais relacionados às questões voltadas à administração do que ao direito. Por isso, para uma boa adequação é necessário que se procure auxílio de uma equipe multidisciplinar, para que se realize um bom inventário dos dados, uma análise dos riscos à proteção e privacidade dos dados e a implementação de controles que mitiguem os possíveis incidentes. Além disso, é importante instituir uma equipe interna de implementação, que conheça de forma clara todos os processos e procedimentos da igreja, a fim de auxiliar na identificação das necessidades de adequação.

Uma vez conhecidos a fundo os processos e procedimentos, deve-se identificar os processos que tratam dados pessoais e inventariar estes dados, indicando todos aqueles princípios que listamos anteriormente e já fazendo a adequação, através de documentação dos controles necessários para evitar incidentes no uso dos dados.

Qualquer dado tratado pela igreja deve estar adequado à LGPD, desde um simples pedido de oração, que coleta dados de pessoas naturais, como o nome e endereço, por exemplo, deve deixar clara a finalidade, a transferência deste dado, como nos casos em que ele será enviado para um grupo de orações, o descarte do dado, ou seja, o que será feito com este dado, mesmo que seja somente um papel com o nome escrito, após o tratamento, e, principalmente a base legal, que, se for o consentimento do titular, temos que ter formas de documentar este, através da manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para esta finalidade.

BOAS PRÁTICAS A SEREM ADOTADAS

•Instruir e treinar os funcionários e obreiros para que eles tenham o hábito de praticar as definições de boas práticas;

•Evitar gravar senhas, computadores sem senhas, acesso total ao conteúdo WEB. Tudo isso pode parecer prático no dia-a-dia, mas gera uma vulnerabilidade enorme no ambiente;

•Aplicar políticas de segurança, a fim de amenizar os riscos de vazamentos e trazer um melhor controle das informações.

•Não acessar páginas na internet, que sejam suspeitas, na rede da empresa;

•Bloquear a estação de trabalho ao se ausentar;

•Não deixar documentos expostos ao se ausentar da estação de trabalho;

•Não fotografar e/ou tirar prints de telas que contenham dados pessoais;

•Implementar uma Políticas de consequências;

•Criar modelos de autorizações para uso de dados pessoais;

•Minimizar dados desnecessários, como aqueles relativos a ex-membros;

•Elaborar a política de proteção e privacidade de dados e incluir no site;

•Informar sobre fotos e filmagens que possam ser feitos e ter um local específico onde as pessoas que não consentirem com o uso de sua imagem possam permanecer, alertando quanto a esta prática, na política;

•Evirar coletar informações desnecessárias em determinados documentos;

•Elaborar uma política de descartes que defina, inclusive, como os dados serão descartados, principalmente aqueles em meio físico;

•Adequar os contratos com terceiros que recebem dados pessoais controlados pela igreja.

DICA.: É impossível ter segurança digital sem o uso de ferramentas adequadas e eficazes. Muitas vezes o investimento em segurança digital é visto como um custo sem retorno, entretanto ao serem analisados os prejuízos por falta de segurança, observa-se que estas ferramentas são parte fundamental e essencial para um ambiente seguro e estável.

IMPLEMENTAR A LGPD DADOS

VANTAGENS EM IMPLEMENTAR A GOVERNANÇA DE DADOS

Além de garantir a conformidade legal, uma boa implantação da governança de dados também traz como benefícios:

•Estruturação e organização dos dados;
•Maior conhecimento da operação;
•Mapeamento e reengenharia de processos;
•Vantagens comerciais (diferencial);
•Segurança do ambiente de TI;
•Preparação do ambiente para implementação da governança corporativa;
•Aumento da confiança de acionistas, parceiros e clientes.

Por fim, considerando o ineditismo deste tipo de legislação no território brasileiro, muita coisa poderá ser alterada na sua regulamentação, porém, é importante começar a jornada de adequação para não ser pego de surpresa, considerando que esta lei já esta vigente desde agosto de 2020 e as sanções administrativas já estarão penalizando as organizações a partir de agosto de 2021. Atualmente, tanto as igrejas, como qualquer outra organização já estão sujeitos aos processos judiciais, os quais já estão acontecendo e, até junho de 2021 já havia mais de 600 decisões envolvendo a LGPD.

VIEIRA & REGINA
SOCIEDADE DE ADVOGADOS

COMPLY LGPD SOLUTIONS

LGPD NAS ORGANIZAÇÕES RELIGIOSAS