LGPD O QUE É OBRIGATÓRIO SABER
para Escritórios de Advogados

COMISSÃO DE ESTUDO E ACOMPANHAMENTO DA LEI GERAL DE PROTEÇÃO DOS DADOS E SEGURANÇA DA INFORMAÇÃO - CEA-LGPD

ORDEM DOS ADVOGADOS DO BRASIL

OAB

MATO GROSSO DO SUL

Produzido pela Comissão de Estudo e Adequação à LGPD da OAB/MS em parceria com o Comissão de Sociedade de Advogados - CSA da OAB/MS Comissão de Proteção e Privacidades de Dados Pessoais - LGPD de Dourados

Sob a Coordenação de
Giuliana Borges Assumpção Gattass

Autores Membros da CEA LGPD:
Diogo Ferreira Rodrigues
Fernando Henrique Baena Alli
Edilson Vargas da Silveira
Jaqueline Nais Inoue
José Francisco de Souza Bezerra Carvalho
Kellyne Laís Laburú Alencar de Almeida
Luiza Carolen Cavaglieri Faccin
Luciano Barbosa de Campos
Maria Gabriela Lordelo de Vasconcelos

Membro da Comissão de Sociedade de Advogados
Renata de Cassia Moraes Nicodemos

Membros da Comissão de Proteção e Privacidades de Dados Pessoais - LGPD da 4ª Subseção
Carlos Henrique Garcia de Medeiros
Maíra Salgueiro Freire

DIRETORIA OAB-MS

Bitto Pereira
Presidente

Camila Bastos
Vice-Presidente

Luiz Rene G. do Amaral
Secretário Geral

Janine Antunes Delgado
Secretária Geral Adjunta

Fabio Nogueira Costa
Diretor-Tesoureiro

Diretoria CAAMS:

Marco Aurélio de Oliveira Rocha
Presidente

Marta do Carmo Taques
Vice-Presidente

Euclydes José Bruschi Júnior
Secretário-Geral

Janaína Pouso Rodrigues
Secretária-Geral Adjunta

Roberto Santos Cunha
Tesoureiro

Diretoria ESA/MS:

Lauane Braz A. Volpe Camargo
Diretor Geral

João Paulo Sales Delmondes
Vice-Diretor Geral

Marcelo Radaelli Da Silva
Secretário Geral

Nabiha De Oliveira Maksoud
Secretária Geral Adjunta

Abner Jaques
Diretor-Tesoureiro

Coordenação Editorial
Valter Jeronymo

Assistente de Coordenação
Alyne Rebeca

Projeto Gráfico
Diagramação e Capa
Life Editora

Revisão
Giuliana Borges Assumpção Gattass

Life Editora
Rua Américo Vespúcio, 255 - Santo Antonio
CEP: 79.100-470 - Campo Grande - MS
Fones: (67) 3362-5545 - Cel.: (67) 99297-4890
contato@lifeeditora.com.br • **www.lifeeditora.com.br**

Dados Internacionais de Catalogação na Publicação (CIP)

OAB-MS Ordem dos Advogados do Brasil Seccional Mato Grosso do Sul

LGPD - O QUE É OBRIGATÓRIO SABER para escritórios de Advogados, OAB-MS. - Campo Grande, MS, Life Editora, 2022.

101p.

ISBN 978-65-5887-136-1

1. Segurança de Dados 2. Proteção de Dados 3. LGPD I. Título

CDD - 340

SUMÁRIO

APRESENTAÇÃO

Após a entrada em vigor da Lei Geral de Proteção de Dados em 18 de setembro de 2020, adequação a nova legislação tornou-se essencial a todos que tratam dados pessoais, com fins econômicos, dados pessoais de clientes, fornecedores, colaboradores, servidores, empregados, parceiros de negócio, etc. seja no formato físico ou no formato digital.

Os advogados diariamente coletam, armazenam, partilham, atualizam, excluem, um grande número de dados pessoais, como instrumentadores do Direito e figuras essenciais à justiça

É fundamental que os escritórios de advogados estejam em conformidade com o conteúdo da LGPD e demais normas que se referem a Proteção de Dados e Segurança da Informação em território brasileiro.

Assim sendo o e-book “LGPD O QUE É OBRIGATÓRIO SABER – Para os Escritórios de Advogados”, é mais uma entrega à sociedade, idealizado pela Comissão de Estudos e Avanço da LGPD da OAB/MS, isto é a concretização de um projeto que contou com o apoio da Co-

missão de Proteção e Privacidades de Dados Pessoais - LGPD de Dourados e da Comissão de Sociedade de Advogados.

O texto da obra foi escrito por diversos membros das três comissões, que somaram esforços com o intuito de ser um pilar estrutural de conscientização e posterior aplicação correta do texto da LGPD nos escritórios de advogados

Os advogados devem utilizar-se dos dados pessoais de forma correta, segura, bem como, cumprir todo o conteúdo normativo em vigor, especialmente a Constituição Federal e a Lei Geral de Proteção de Dados, com ética, integridade, transparência e boa-fé.

Os autores, no presente trabalho, não objetivaram exaurir o tema, nem tão pouco substituir as orientações da Autoridade Nacional de Proteção de Dados – ANPD. Antes, procuraram mais uma vez partilhar conhecimentos, com caráter informativo, através de um texto claro, objetivo e útil, para facilitar a compreensão e a aplicação do texto normativo, diante dos inúmeros questionamentos, dúvidas e desafios diários

É necessário ter consciência que não há mais tempo a perder e todos os escritórios de advogados precisam estar em conformidade com o texto da LGPD.

Boa Leitura!

Giuliana Borges Assumpção Gattass
Presidente da CEA LGPD

1. ASPECTOS GERAIS DA LGPD?

Por Giuliana Gattass

A sigla LGPD refere-se à Lei 13.709/2018, Lei Geral de Proteção de Dados, que entrou em vigor no dia 18 de setembro de 2020, para preencher lacunas e substituir mais de 30 diplomas legais que, de forma esparsa, regulamentavam o uso de dados no Brasil, como o Código de Defesa do Consumidor (Lei nº. 8078/90), Lei do Cadastro Positivo (Lei nº. 12.414/2011), Lei de Acesso à Informação (Lei nº. 12.527/2011) e Marco Civil da Internet (Lei nº. 12.965/2014).

A LGPD foi a primeira norma a tratar direta e exclusivamente do tema, além de unificar importantes conceitos, princípios, obrigações, direitos e sanções pelo seu descumprimento.

O legislador brasileiro seguiu a mesma direção normativa do Regulamento Geral de Proteção de Dados - GPDR - vigente na Europa e redigiu uma norma que protege os dados tanto físico como digitais, em qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou priva-

do, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

A LGPD visa, sobretudo, proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural. Estes alicerces merecem elevada atenção, especialmente considerando que vivemos em uma sociedade da informação cada vez mais movida por dados tanto no contexto físico como digital, os quais ainda são muitas vezes indevidamente e ilicitamente utilizados.

A norma não prevê sanções penais no caso de descumprimento, somente sanções administrativas e cíveis.

2. POR QUE DEVO ADEQUAR MEU ESCRITÓRIO?

Por Giuliana Gattass

A extensão dos efeitos da lei 13.709/2018, a Lei Geral de Proteção de Dados, aos advogados tem sido tema recorrente no meio jurídico.

Alguns advogados ainda entendem que pouca coisa mudaria o cotidiano do escritório com a entrada em vigor da LGPD, em face da relação jurídica entre cliente-advogado ser embasada no sigilo profissional.

De fato, o sigilo profissional do advogado, termos do Código de Ética e Disciplina da OAB (art. 25), inerente ao exercício da advocacia., em certa medida, pode ser considerado até mais amplo e rígido do que as regras impostas pela LGPD para o tratamento de dados pessoais.

Em contrapartida, porém, o dever de sigilo profissional determina apenas que o advogado mantenha sigilo sobre toda e qualquer informação dos seus clientes que tenha acesso. Não há regras que especificam quais dados o advogado pode acessar, por quanto tempo ou ainda em que condições deve guardá-los, entre tantas outras regras agora trazidas pela LGPD.

Todo e qualquer cliente quando recorre aos serviços de um escritório de advogados, deposita ali toda a sua confiança na equipe contratada e fornece a ela um grande número de informações para que os seus interesses possam ser defendidos. Importante destacar que, tais informações normalmente englobam diversos dados pessoais inclusive nos meios digitais e muitas vezes dados sensíveis ou ainda dados de crianças e adolescentes, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

Diante do texto do artigo 3º, II LGPD, não resta dúvida de que todos os escritórios de advogados precisam estar em conformidade com o texto da LGPD.

Enganam-se aqueles que acreditam que a norma se aplica única e exclusivamente às empresas. Todas as pessoas jurídicas e inclusive pessoas naturais (física), sejam elas de direito público ou privado que tratem dados pessoais, sejam eles de funcionários ou colaboradores, fornecedores, sócios ou clientes, seja anotando num caderno/papel ou pela via digital, deverão seguir o que determina o texto da lei, e deverão corrigir dados pessoais incompletos, inexatos ou desatualizados, efetuar bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei, permitir e portabilidade de dados a outro

fornecedor de produto ou serviço, além de eliminar dados tratados sem consentimento.

O art. 4º da LGPD prevê que as exceções a aplicabilidade da lei, a qual não se aplica ao tratamento de dados pessoais: realizado exclusivamente por pessoa natural para objetivos particulares/não econômicos; para fins jornalístico e artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais, devendo ser aprovada legislação especial para tais situações; ou 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 nesta Lei.

A adequação pode trazer algumas vantagens aos escritórios de advogados como:
1. Conhecer as vulnerabilidades (físicas e digitais) da estrutura, especialmente no tocante a segurança da informação;
2. Entender a verdadeira realidade da vida útil dos dados que são tratados pelo escritório;

3. Aumentar a consciência sobre a segurança da informação de todos integrantes;
4. Identificar e proteger os dados já existentes, bem entender onde eles estão armazenados;
5. Maior Credibilidade do escritório;
6. Melhoria no Nível de responsabilidade dos integrantes da equipe;
7. Maior clareza no controle de acesso às informações;
8. Evitar sanções administrativas e ações judiciais.

No caso de descumprimento ao texto legal ou no caso de vazamento de dados poderão ser aplicadas sanções na esfera administrativa que vão desde uma advertência, o bloqueio de dados pessoais, a suspensão temporária ou a proibição da atividade de tratamento de dados pessoais até a aplicação de multa simples de até 2% do faturamento no seu último exercício, excluídos os tributos, limitada a R$ 50.000.000,00 por infração e ainda multa diária, respeitado o limite do da LGPD e ainda poderão ser aplicadas também sanções na esfera do poder judiciário.

3. DESAFIOS E IMPACTOS DA LGPD NA ROTINA DOS ESCRITÓRIOS DE ADVOCACIA

Por Renata de Cassia Moraes Nicodemos

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, se aplica a qualquer seguimento e qualquer atividade desenvolvida com uso de dados pessoais, em território brasileiro e com fins econômicos. Neste texto, serão abordados aspectos que demonstram os desafios e impactos dessa norma para os escritórios de advocacia.

Em verdade, vale ressaltar que desde a vigência da mencionada lei, ficou evidente a necessidade de construção de uma política de governança em privacidade e o desenvolvimento de diretrizes para o armazenamento e tratamento de dados pessoais.

Os escritórios de advocacia não ficaram imunes à obrigatoriedade de adequação, submetidos ao que foi a uma profunda mudança na rotina, o art. 3º[1] da referi-

1. "LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados(...)."

da lei não deixa dúvidas da extensão dos seus efeitos.

A criação de uma norma específica, corrobora a necessidade de construir uma cultura de valoração da privacidade, a exemplo do que ocorreu no passado em relação aos direitos individuais relativos às relações de consumo. Em outras palavras, a proteção dos dados não pode ser analisada de forma isolada, pois está diretamente ligada a cultura da sociedade.

Nessa perspectiva, é essencial refletir quais as regras de negócio próprias para assegurar o cumprimento da lei. Pois bem, a existência de fluxos multidimensionais na rotina dos escritórios de advocacia, confere maior desafio no processo de adequação. Por exemplo, para cumprir a rotina de análise de processos, petições, atendimento de consultas, reuniões com clientes, audiências, dentre outras, ocorre de alguns escritórios adotarem procedimentos e ferramentas frágeis a assegurar a privacidade das informações.

Outrossim, não é rara a contratação de advogados particulares para tratar as atividades que não estão sob o páreo celetista ou de sócio da banca a quem foi conferida a procuração, o que pode culminar na transferência

de informações de maneira insegura, se não observadas as regras de confidencialidade e tratamento dos dados. Levando em conta os princípios traçados na Lei, é fácil perceber que o contexto da LGPD não é somente proteger os dados, mas está diretamente ligado a privacidade.

Neste aspecto, é importante mencionar que código de ética e disciplina da OAB traz em seu artigo 25, a defesa ao sigilo profissional como forma de garantir o livre exercício da profissão, o que não se confunde com a proteção de dados em virtude a relação de negócio estabelecida entre as partes.

Isto quer dizer que ao repassar dados para o advogado o cliente está protegido pelo sigilo profissional, entretanto, se esse advogado disponibilizar essa informação em software, por exemplo, é importante ter atenção com relação ao sigilo perante terceiros, tendo em vista a relação negocial entre as partes.

Sob o prisma mercadológico o instituto atingiu sobremaneira a relação negocial, visto que os clientes passaram a exigir a maior atenção com a privacidade de seus dados. Assim, o que antes era considerado apenas boas práticas e diferencial competitivo, hoje passa

a ser obrigação legal e requisito para posicionamento diante do mercado.

Nessa perspectiva, é fácil perceber que o tratamento de dados pessoais está presente em muitas atividades do cotidiano dos escritórios de advocacia, seja na relação com seus clientes, com seus colaboradores, em novas contratações, ou até mesmo, na prospecção de novos clientes.

Por isso, para construção de uma política de privacidade é necessária a atenção a algumas etapas, dentre as quais: a) identificação da atividade desenvolvida; b) identificar quem são os titulares de dados (clientes, partes dos processos, funcionários, colaboradores, crianças e adolescentes); c) identificar a finalidade dos dados; d) definição do ciclo de vida desses dados; e) definição das bases legais; f) estabelecer medidas de mitigação de risco.

É dever afirmar que o processo de adequação é relativamente complexo e envolve uma ampla revisão das políticas de segurança e adoção de novos procedimentos, pois todas as atividades hoje desempenhadas deverão passar por algum tipo de conformidade ou adaptação.

Percebe-se, outrossim, a importância dos escritórios trabalharem internamente sua cultura organizacional e adotarem importantes medidas para mitigar os riscos, quais sejam: a) atualização da procuração para conter máxima especificação do escopo e quando trabalhar um fluxo alicerçado no consentimento que as disposições sejam claras e específicas; b) inserção de cláusula de confidencialidade das informações no contrato com os colaboradores; c) na prospecção e divulgação de boletins e notícias, certificar a base legal adequada (geralmente o consentimento ou o legítimo interesse), bem como a adoção de medidas de transparência; d) inclusão de cláusulas de proteção nas novas contratações e identificação do tipo, fim específico e o nexo causal; e) implantar política de segurança da informação; f) nomear os responsáveis para condução dos processos de adequação; g) solicitar parecer técnico acerca da vulnerabilidade de segurança dos dados, seja para equipe de TI ou para os Softwares; h) mapear os fatores de risco e executar um plano de ação imediato, de modo a evitar o vazamento de dados; i) verificar os níveis de permissão, se o acesso está adequado à finalidade ; j) buscar sempre a digitalização, estabelecendo política de retenção de dados de modo a evitar o acúmulo de informações obsoletas.

Não se deve esquecer que em verdade, qualquer escritório de advocacia detém um grande número de dados sensíveis. A conclusão é simples: é exigível dos escritórios que tenham a segurança necessária para manuseio dos dados, uma vez que não pode ser alegado o desconhecimento da lei.

É importante ter a clareza das sanções em caso de desconformidade legal, as quais variam entre sanções administrativas, condenações judiciais, multas contratuais e, a pior delas, um considerável impacto na reputação profissional.

De acordo com o regramento legal, haverá muito mais do que a necessidade de processos estruturados, mas também a necessidade de promover gestão e transformar a cultura do meio. O maior desafio a ser enfrentado refere-se à cultura do escritório e, neste particular, é necessário abstrair conceitos e treinar exaustivamente os colaboradores para conferir a segurança.

Não se pode deixar de considerar que o caminho da conformidade à LGPD não tem uma reta de chegada. É um processo continuado, portanto, tão importante quanto estar conforme é se manter conforme.

Indiscutivelmente, a adequação a LGPD é, para o modelo atual dos escritórios de advocacia, o caminho árduo, mas necessário, para segurança dos dados. É razoável afirmar que esse processo será mais fácil se os escritórios estiverem familiarizados com os conceitos, objetivos e peculiaridades da lei.

Por fim, percebe-se, com isso, que não existe um roteiro preciso a ser seguindo, mas a privacidade dos dados é um caminho sem volta e cada escritório terá seus próprios desafios.

CONCEITOS ESSENCIAIS PARA ADEQUAÇÃO

4. CONCEITOS ESSENCIAIS PARA ADEQUAÇÃO

a) Dados pessoais

Por Giuliana Gattass

Os dados pessoais são as informações relativas a pessoa, que permitem sua identificação, ou, como consta da LGPD "informação relacionada à pessoa natural identificada ou identificável".

A LGPD adota a ideia de que dado pessoal é toda informação que pode tornar uma pessoa identificada ou identificável, todo e qualquer dado que possa ser associado a um indivíduo, fazendo com que a aplicação da norma esteja concentrada nos direitos e no poder que o indivíduo tem sobre o seu próprio dado.

Os dados podem ser classificados em
- dados pessoais;
- dados sensíveis;
- dados anonimizados e pseudonimizados;
- dados de crianças e adolescentes.

Os dados que são protegidos pela lei são aqueles que podem ser coletados tanto offline ou online, offline são todos aqueles que podem ser coletados pelos meios físicos, não digitais, quando preenchemos uma ficha no consultório médico, preenchemos aquele papel para concorrer ao sorteio de Natal no Shopping, fornecemos nosso CPF na farmácia.

E dados coletados online ou pelos meios digitais são aqueles que fornecemos quando utilizamos uma rede social, um aplicativo de conversa, um banco virtual, buscas no Google.

Os dados pessoais ainda podem identificar alguém de forma direta ou indiretamente. Os que permitem identificar diretamente são aqueles que por si só permitem identificar o seu titular, sem a necessidade de ser utilizado em conjunto com outro dado como é o caso do RG, CPF, Título de Eleitor, matrícula da universidade, CTPS.

Já os que permitem identificar indiretamente são aqueles que conseguem identificar o titular dos dados somente se forem utilizados em conjunto com outras informações como: data e local de nascimento, endereço residencial, localização via GPS, endereço de

IP (Protocolo da Internet), profissão. Não são exclusivamente relacionados a uma única pessoa, podem ser utilizados para identificar mais de uma pessoa se usados isoladamente.

Podemos identificar uma pessoa de modos indireto como num exemplo hipotético:
- quantos advogados temos no Brasil?
- quantos estão inscritos na OAB/MS?
- quantos na cidade de Campo Grande/MS?
- quantos trabalham efetivamente com proteção de dados?
- quantos são da Diretoria da CEA LGPD?
- quantos do sexo feminino?
- E são loiras?

Uma forma de identificação que a princípio parecia ser com repleta de dados anonimizados[2], porém na verdade foram utilizados diversos dados quantitativos até que fosse possível identificar indiretamente o titular do dado.

A LGPD aborda ainda os dados sensíveis e os dados de crianças e adolescentes.

2. A anonimização de um dado é o processo no qual a informação pertencente a uma pessoa deixa de ser capaz de identificá-la ou torná-la identificável, e, portanto, deixa de ser considerado dado pessoal por força de lei.

b) Dados pessoais sensíveis e dados de crianças e adolescentes

Por Giuliana Gattass

De acordo com o texto normativo dado pessoal sensível é todo aquele 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 (inciso II, do art. 5º da LGPD).

O rol constante na LGPD acerca dos dados sensíveis é taxativo, ou seja, não permite interpretações extensivas.

Os dados sensíveis são aqueles que além de identificar também qualificam os seus titulares, de modo mais íntimo, que usados de forma inadequada podem gerar constrangimento, discriminação ou até mesmo perseguição em razão de crença religiosa, escolha política, característica física do seu titular, por isso exige exigindo um regime jurídico diferenciado.

Já em relação aos dados de crianças e adolescentes é importante entender a diferença entre as definições de criança e de adolescente, estabelecidas pelo ECA.

- Criança: tem até doze anos incompletos;
- Adolescente: tem entre doze e dezoito anos de idade.

A proteção da privacidade de crianças e adolescentes merece uma reflexão e por isso, e um ambiente regulatório que permita a proteção de crianças e adolescentes, particularmente, considerando a crescente e inevitável imersão desse grupo no mundo digital.

Para garantir a proteção e a privacidade das crianças e adolescentes, a LGPD determina que o tratamento de dados pessoais de crianças e adolescentes deverá ser sempre em seu melhor interesse. E ainda que é obrigatório o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Além disso, a lei determina que o controlador deve realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança ou adolescente.

Dados pessoais de crianças e adolescentes, poderão ser coletados sem o consentimento do responsável somente em duas situações: quando a coleta for necessária para contatar os pais ou responsável legal ou para a proteção da criança. Em nenhum caso os dados podem ser repassados a terceiros sem consentimento.

As informações sobre o tratamento de dados de crianças e adolescentes devem ser elaboradas de maneira simples, clara e acessível, "de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

c) Controlador

Por Giuliana Gattass

O controlador é o agente de tratamento de dados responsável por estabelecer as principais diretrizes, tomar as principais decisões no tocante ao tratamento dos dados pessoais, como definir quais os dados devem ser coletados, a finalidade da coleta de cada um deles e a base legal, quanto tempo deverão ser armazenados. Portanto, detém a obrigação de fornecer as instruções aos operadores, agentes de tratamento contratados,

para a execução de um determinado tratamento de dados pessoais.

O artigo art. 5º, VI, da LGPD define controlador como: "Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais."

O controlador será pessoa jurídica, tanto de direito público quanto privado, quando tomar as principais decisões a respeito do tratamento de dados dentro da sua organização.Já o controlador pessoa natural, ou também chamado de pessoa física, age em nome próprio, de forma independente, neste âmbito encontram-se empresários individuais, profissionais liberais, além dos responsáveis pelas serventias extrajudiciais.

Importante destacar que o controlador não precisa necessariamente ter acesso aos dados ou processar os dados, mas deve tomar as principais decisões sobre os tratamentos a serem executados.

O escritório será considerado controlador nas relações em que determina as regras do tratamento de dados, tem o poder de definir quais os dados serão tratados, como

por exemplo quando contrata uma empresa para criar o site do escritório, uma empresa para gerir o marketing, quando coleta dados para a execução de contratos com fornecedores, na relação de trabalho com colaboradores ou para controle de acesso às suas dependências, são tratados na condição de controlador. Assim, enquanto controlador, o advogado terá uma responsabilidade mais abrangente, pois caberá a ele definir todos os aspectos relacionados aos dados recebidos para tratamento.

d) Operador

Por Giuliana Gattass

O Operador é a pessoa que executa e trata o dado a mando do controlador. O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este definida.

A definição legal se encontra no art. 5º, inciso X da LGPD:
"Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador."

Nesse mesmo sentido é a previsão do art. 39 da LGPD: "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 previsão acima implica dizer que o operador não tem a liberdade para tomar decisões importantes no que se refere ao tratamento de dados e só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador.

Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador. Somente toma decisões meio, isto é, não essenciais (como por exemplo em relação a software, hardware, antivírus a ser adotado).

Importante destacar que os advogados correspondentes, os quais recebem as orientações sobre o que devem fazer e não possuem liberdade de escolha ou poder no tocante a tomada de decisão, poderão ser considerados como operadores, quando atuarem no apoio e sob as regras impostas pelo escritório controlador.

Ressalta-se aqui o artigo 42 da LGPD, o qual determina a responsabilidade solidária do controlador e operador por eventuais danos causados ao titular de dados.

e) Tratamento de dados

Por Edilson Vargas da Silveira

O tema privacidade e proteção de dados pessoais, a princípio parece novo, porém, não é não tão recente assim, pois a primeira lei sobre o tema surgiu na Alemanha, ainda em 1970, em pleno século XX. O tema despertou o interesse de muitos estudiosos do direito e foi muito debatido em diversos países, provocando sua expansão pelo mundo , até que, em 2012, surge na Europa o GDPR (General Data Protection Regulation), ou o Regulamento Geral sobre a Proteção de Dados.

No Brasil, nossa Lei de Proteção de Dados E Segurança da Informação, entrou em vigor em 2020, o legislador brasileiro inspirou-se no modelo da GDPR da Europa.

É importante destacar que a Lei 13.709/18 refere-se ao tratamento de dados pessoais, tanto nos meios físicos quanto nos meios digitais, por pessoa física ou jurídica,

de direito público, ou privado, sempre com o escopo de proteger os direitos fundamentais da liberdade e de privacidade do titular de dados, bem como, o livre desenvolvimento da personalidade natural do cidadão.

Sendo assim, as normas gerais contidas na Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

O termo "tratamento de dados" refere-se a toda e qualquer atividade que sutilize um dado pessoal na execução da uma operação, como por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Dessa forma, o "tratamento dos dados pessoais" deverá ser realizado por dois agentes de tratamento, na conformidade com artigo 5º, da Lei 13.709/2018: o controlador, a quem compete as decisões referentes aos tratamentos de dados pessoas e figura do operador, que realiza o trabalho operacional de tratamento de dados pessoais, em nome do controlador.

Os agentes de tratamentos de dados devem resguardar alguns princípios fundamentais no tratamentos de dados, quais sejam :

1. Princípio da Licitude, Lealdade e Transparência, onde o processamento devem respeitar que a operação de tratamentos seja de forma legal ao que estabelece a lei;
2. Princípio da Limitação da Finalidade: onde os dados devem ser coletados para fins específicos, explícitos e legítimo;
3. Princípios da Minimização dos Dados: os dados coletados devem ser adequados relevantes e limitados aos necessários em relação aos fins para os quais são processados;
4. Princípios da Exatidão: Neste princípio os dados devem ser precisos e de preferência sempre atualizados;
5. Princípios da Limitação ao Armazenamentos: este princípio congrega que os dados colhidos devem manter-se em armazenamento não mais do que o necessário e o fim pré-estabelecido no consentimento, armazenados em formatos que permita a identificação dos titulares dos dados;
6. Princípio da Integridade e Confidencialidade: os dados pessoais armazenados devem garantir a segurança da informação.

Portanto, a Lei de Proteção de Dados - LGPD - exige


CICLO DE VIDA DOS DADOS
Eliminação
Coleta
Reutilização
LGPD
Art. 5º
Processamento
Armazenamento
Análise
Compartilhamento

que todo documento que contenha dado pessoal tenha definido um ciclo de vida, ou seja, que a empresa deve processar, armazenar e após o término da sua finalidade, excluir ou armazenar esse material, caso seja necessário.

f) Bases legais na Lei Geral de Proteção de Dados

Por Luiza Carolen Cavaglieri Faccin

A Lei trouxe bases legais para o tratamento dos dados, ou seja, determinou em quais ocasiões os dados poderão ser tratados.

As bases Legais para o tratamento dos dados estão previstas no art. 7º da LGPD. Basta o atendimento de uma das dez bases para o tratamento ser considerado legítimo (sendo possível cumular bases legais dentro de uma mesma atividade, considerando diferentes dados pessoais)[3]

As bases legais não têm dependência ou predominância entre si. Não há que se falar em base legal melhor ou

3. MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. LGPD: lei geral de proteção de dados comentada. São Paulo: Revista dos Tribunais, 2019.

pior, a análise que se faz é uma de cabimento em relação à realidade do caso. A escolha a respeito do uso de uma determinada base legal dependerá essencialmente das atividades realizadas pelo controlador de dados pessoais, após passar por uma reflexão em concreto, a partir das características particulares dos dados pessoais tratados e das finalidades para tratamento.

Explicamos, de forma direta e descomplicada as 10 bases legais para o processamento válido do tratamento dos dados:

1 – Consentimento:
A Lei Geral de Proteção de Dados estatui que o consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Desta forma, autorizações genéricas ou que não tenham por escopo uma finalidade *específica, explícita e informada* serão nulas.

Segundo a Lei, consentimento é a *"manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"* (art. 5º, XII), ou seja, é a manifestação do próprio titular concedendo o uso, nos ter-

mos legais, de seus dados. Por exemplo, quando este titular aceita, de livre e espontânea vontade, a política de privacidade do site, aplicativo etc.

O consentimento deverá ser fornecido por escrito em cláusula destacada ou por qualquer outra ação afirmativa que demonstre a vontade do titular dos dados. O consentimento implícito não é possível!

O consentimento será sempre considerado uma autorização temporária porque pode ser revogado a qualquer momento pelo titular dos dados pessoais, por procedimento gratuito e facilitado. Importante destacar que na eventualidade de mudança na finalidade do tratamento para a qual o consentimento foi dado, e havendo incompatibilidade entre a mudança e o consentimento originário, o controlador deverá informar previamente o titular dos dados sobre a mudança.

Para os Agentes de tratamento de dados é importante manter uma forma de gerenciamento deste consentimento, pois hoje o titular pode estar muito feliz com a sua forma de tratar seus dados, contudo amanhã ele poderá acordar e simplesmente não lhe conceder mais acesso ao tratamento de seus dados pessoais.

Note, portanto, como o consentimento é volátil e, por isso, é de suma importância gerenciar o consentimento.

2 – Legítimo interesse:
Legítimo interesse é a base legal para tratamento de dados contida no artigo 7º, IX, da LGPD. É uma base legal largamente utilizada – por conta de sua plasticidade e adaptabilidade a variados cenários.

O dispositivo da LGPD que parametriza a aplicação do legítimo interesse como base legal é o art. 10, cujo texto dispõe:
Art. 10. 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 desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garan-

tir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º 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.

O artigo fala em "finalidade" e "interesse". A finalidade é o propósito específico do tratamento de dados pessoais, enquanto o interesse é o valor mais amplo que um tratamento de dados pessoais representa para o seu controlador (ou terceiros, ou a sociedade como um todo). Um interesse, portanto, seria a garantia da segurança e da saúde de um determinado grupo de pessoas, enquanto uma finalidade seria determinado tratamento de dados que garante tal interesse[4].

Mas o que seria um *interesse legítimo*?
Primeiramente, esse interesse deve ser legal, isto é, deve respeitar todas as leis e normas infralegais aplicáveis àquela situação específica. A coleta deve ser relacionada a uma situação concreta e, portanto, não especulativa (que decorre do próprio princípio da fina-lidade).
Bruno Bioni ilustra tal requisito ("legítimo") com o

4. FONTE: ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014.

exemplo da proibição à coleta, mesmo com consentimento, de dados relacionados a gravidez ou HIV em situações de trabalho[5].

O artigo 10 tem por escopo promover o balanceamento dos interesses do controlador ou de terceiros frente aos do titular.

Colocando em prática as técnicas de hermenêutica jurídica sobre a interpretação do art. 10 da LGPD, podemos dizer que o dispositivo (i) refere-se tanto ao legítimo interesse do controlador, quanto de terceiros e que (ii) a relação de incisos e parágrafos do artigo impõe condicionantes cumulativas e não alternativas.

O que isso significa? Que o legítimo interesse, por conseguinte, não é aplicável apenas ao controlador, mas também à figura do "terceiro". Ou seja, o controlador pode realizar um tratamento de dados que não seja no seu próprio interesse (ou exclusivamente no seu próprio interesse), mas no de terceiros ou da sociedade como um todo – por exemplo, evitar que o cartão de crédito que o Banco nos oferece seja fraudado é in-

5. BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2a edição): capítulo 5.

teresse tanto do Banco quanto do sistema bancário e financeiro, bem como da sociedade. (A lei brasileira não traz uma definição de quem seria o "terceiro", nem quando este se enquadra na figura de recipiente, de modo que é ainda mais desafiador interpretar o alcance da base legal do legítimo interesse de terceiro na LGPD, e é tarefa urgente da Autoridade Nacional de Proteção de Dados (ANPD) endereçar a questão.)

O legítimo interesse é, a priori, um conceito jurídico abstrato e indeterminado. É uma hipótese flexível cujo conteúdo e limites não são determinados de início e sua caracterização depende da avaliação de sua conformidade. Em razão desse alto grau de abstração, a legislação impõe a necessidade de que os agentes de tratamento demonstrem que existe um equilíbrio entre os interesses do controlador e a expectativa de privacidade do titular.

Esse equilíbrio é demonstrado por meio de um "teste de proporcionalidade" que pondera entre os objetivos negociais do controlador e as medidas tomadas para a salvaguarda dos direitos do titular. Essa avaliação é registrada em um documento intitulado *"Legitimate Interest Assessment (LIA)*" ou "Avaliação de Legítimo Interesse". Infere-se, portanto, que o ônus argumentativo de que o

interesse é, de fato, *legítimo* pertence sempre ao Controlador de Dados. Logo, é ele quem deverá demonstrar, por meio do teste de ponderação, que existe real legitimidade de seu interesse para a coleta de dados.

O artigo 10 da LGPD estabelece que o legítimo interesse do controlador somente poderá fundamentar o tratamento de dados para finalidades legítimas consideradas a partir de situações concretas. O dispositivo traz um breve rol exemplificativo que engloba o *"apoio e promoção das atividades do controlador e a proteção do exercício regular dos direitos dos titulares ou a prestação de serviços que o beneficiem, respeitadas as legítimas expectativas e direitos fundamentais"*. Note que a expressão "apoio e promoção das atividades" é ampla e pode abrir margem para a utilização do legítimo interesse para o tratamento de dados com as mais diversas finalidades, inclusive publicitárias. O respeito às legítimas expectativas funciona como óbice para que não seja violada a confiança que o consumidor deposita no fornecedor-controlador de dados e relaciona-se com os motivos da contratação[6] .
Uma regra básica para a utilização dessa base legal é

6. OLIVEIRA, Ricardo; COTS, Márcio. O legítimo interesse e a LGPDP. 2 ed. São Paulo: Thomson Reuters Brasil, 2021.

que ela não é aplicável para o tratamento de dados pessoais sensíveis (art. 11 da LGPD).

Mas será que os deveres exigidos para a utilização da base legal do legítimo interesse também se aplicam a microempresas e a empresas de pequeno porte?

Os deveres documentais e procedimentais referentes à utilização da base legal do legítimo interesse, a princípio, direcionado a todos os modelos de negócio, isto é, são horizontais. Porém, não se pode negar que um dos objetivos centrais da LGPD é harmonizar a proteção de dados pessoais dos titulares ao desenvolvimento econômico e à inovação.

A ANPD já publicou, em outubro de 2021, um Guia Orientativo[7] sobre Segurança da Informação para agentes de pequeno porte e, em 28.01.2022, a Resolução CD/ANPD Nº 02, que aprova o regulamento de aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) para agentes de tratamento de pequeno porte. No art. 9º da Resolução CD/ANPD Nº 02, a ANPD autoriza que os agentes de tratamento de pequeno porte cumpram *de forma simplificada* a obrigação de elaboração e ma-

7. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf

nutenção de registro das operações de tratamento de dados pessoais (constante do art. 37 da LGPD).

Portanto, é possível que a ANPD[8] delimite futuramente um regime normativo específico para esse grupo de empreendimentos, podendo incluir questões procedimentais mais brandas também no que toca ao legítimo interesse.

3 – Cumprimento de obrigação legal ou regulatória

Caso exista determinação legal, seja em lei federal, seja em lei estadual ou municipal ou até nas demais normas (decretos, resoluções, portarias etc), o controlador poderá realizar o tratamento de dados pessoais com fulcro nessa base legal.

Essa base legal autoriza que a LGPD não entre em conflito com outras normas vigentes. Assim, mesmo após o encerramento do vínculo que originou o tratamento dos dados, é permitido armazenar dados pessoais em função do cumprimento de obrigações do ordenamento jurídico (legislação trabalhista ou previdenciária,

8. Conforme disposto pelo art. 55-J, XVIII, da LGPD, é competência da Autoridade Nacional de Proteção de Dados editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que esses modelos de negócios (microempresas e a empresas de pequeno porte) possam se adequar à lei.

Lei de Acesso à Informação - Lei nº 12.527/2011, Lei do processo administrativo na administração pública federal, Marco Civil da Internet - Lei nº 12.965/2014 etc), em função de investigações criminais tributárias, cíveis, contábeis ou administrativas, entre outros.

Obrigações assumidas por ocasião de relações privadas ou contratos não são acobertadas por esse inciso.

Existe a possibilidade de estender o entendimento dessa base legal às determinações previstas na legislação internacional ou nas melhores práticas comprovadamente seguidas por determinado nicho da indústria[9] .

4 – Tratamento pela administração pública

Essa base legal autoriza que a administração pública faça 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.

É claro que o Poder Público deverá informar a finalida-

9. MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. LGPD: lei geral de proteção de dados comentada. São Paulo: Revista dos Tribunais, 2019.

de e a forma como o dado será tratado, respeitando os fundamentos da LGPD, ainda que o consentimento não seja requisito para que seja feito o tratamento.

Adicionalmente, o ente público deve necessariamente atentar-se a todas as demais regras e responsabilidades previstas nos artigos 23 a 32 da LGPD, que detalham extensivamente o que deve ser levado a efeito para o tratamento de dados pelo Poder Público.

5 – Realização de estudos e pesquisas

Ao trazer essa hipótese, o legislador permite que os dados pessoais sejam utilizados sem consentimento em pesquisas de caráter tecnológico, estatístico e/ou histórico.

Nunca é demais lembrar que a autorização só se aplica quando o estudo é conduzido pelo que se entende como órgão de pesquisa, cuja definição está expressamente descrita na própria Lei Geral de Proteção de Dados (art. 5, VIII):

XVIII - 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;

Apesar de não se tratar de conduta obrigatória, a lei recomenda que os dados sejam anonimizados nesses casos.

6 – Execução ou preparação contratual

Trata-se de hipótese em que o tratamento dos dados pessoais é indispensável ao procedimento que antecede a formalização de instrumento contratual, bem como à própria execução das obrigações contratualmente firmadas.

Entre os exemplos mais comuns, estão os levantamentos realizados por instituições financeiras para concessão de crédito e a coleta de dados pessoais para formalização de contrato com o objetivo de adquirir produtos ou serviços.

Por óbvio, é necessário que o próprio titular dos dados tenha sinalizado previamente o interesse na relação estabelecida, limitando-se o tratamento dos dados fornecidos à finalidade proposta.

7 – Exercício regular do Direito:
Aqui o Legislador trouxe uma segurança aos Agentes de Tratamento de Dados, assegurando que o tratamento de dados pode ser feito independente do consentimento do titular, quando este tratamento for para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Assim, a Legislação busca esclarecer que a proteção dos dados pessoais não pode interferir no direito em que as partes têm de produzir provas em processos judiciais, uma contra as outras.

Pense em uma empresa que sofre uma ação por suposta negativação indevida e fica impossibilitada de apresentar uma prova de negativações anteriores do autor, nos termos da súmula 385 do STJ, pois no extrato de negativação estão os dados do autor.

Desta forma, tal base legal garante às partes o direito ao contraditório e ampla defesa sem incorrer em risco de infringir alguma regra da Lei Geral de Proteção de Dados.

Podem ser utilizados como parâmetro para retenção da informação os respectivos prazos prescricionais

previstos na legislação civil e penal. Ou seja, havendo discussão judicial, haverá fundamento para armazenamento dos dados durante todo o prazo em que subsistir possibilidade de discussão da demanda.

8 – Proteção da vida e da incolumidade física
Neste caso, o legislador possibilita utilização de dados pessoais sem consentimento quando a vida ou a segurança física (do titular e/ou de terceiros) estiver em risco.

Trata-se de hipótese relacionada a questões especificamente graves, sendo tal critério restritivo e somente aplicável quando as circunstâncias forem constatadas, de fato.

Entre as possíveis aplicações, está a utilização de dados de geolocalização de dispositivos móveis para localização de vítimas de incidentes.

9 – Tutela de saúde do titular
O legislador também elenca como hipótese o tratamento de dados com o objetivo específico de proteção à saúde.

Trata-se da base legal que fundamenta e justifica a atuação de profissionais da área da saúde (médicos, biomédicos, nutricionistas, psicólogos, enfermeiros,

farmacêuticos, fisioterapeutas, educadores físicos, entre outros) e entidades membro do SNVS (Sistema Nacional de Vigilância Sanitária) no tratamento de dados contidos – por exemplo – em prontuários, exames, prescrições, termos de consentimento e sumários de transferência. Também é o caso da análise de dados necessária para uma campanha de vacinação ou para notificar um paciente sobre o resultado de um exame.

10 – Proteção de crédito

Trata-se do fundamento legal para consulta de informações sobre adimplência e inadimplência, essa realizada para fins de concessão (ou não) de crédito ao titular dos dados.

Cumpre sempre frisar a necessidade de compatibilização desta base legal com as normas já postas, entre elas a Lei do Cadastro Positivo (Lei n. 12.414/2011) e o Código de Proteção e Defesa do Consumidor (Lei n. 8.078/1990).

O fato de existirem dados pra amplo acesso não retira a proteção que a eles deve ser concedida. Mesmo os dados que estejam publicamente acessíveis, por meio físico ou virtual, somente poderão ser tratados caso observados os princípios da finalidade, da boa-fé e do interesse público.

g) Encarregado de proteção de dados.

Por Maria Gabriela Lordelo de Vasconcelos

A profissão de encarregado de dados pessoais ou DPO - data protection officer não é somente uma profissão nova como também se destaca como uma das mais promissoras do momento

Nos termos da LGPD, Encarregado pela Proteção de Dados Pessoais é a 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).

As funções do Encarregado, ou no termo inglês Data Protection Officer (DPO), 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.

Cumpre ressaltar que o encarregado pode ser pessoa física ou jurídica devendo ser uma obrigação de indicação pelo controlador e operador tendo a sua identidade e informações de contato divulgadas de forma clara e objetiva, salvo que a ANPD disponha sobre dispensa de obrigatoriedade conforme art. 41 da LGPD.

h) Titulares de dados e seus direitos

Por José Francisco de Souza Bezerra Carvalho

O titular dos dados pessoais é toda pessoa natural a quem se referem os dados que são objeto de tratamento. Nos termos do art. 17 da LGPD, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Isso significa que, ao permitir o tratamento de seus dados pessoais, de modo algum e em nenhuma circunstância, a pessoa transfere a outrem a condição de dono de seus próprios dados pessoais.

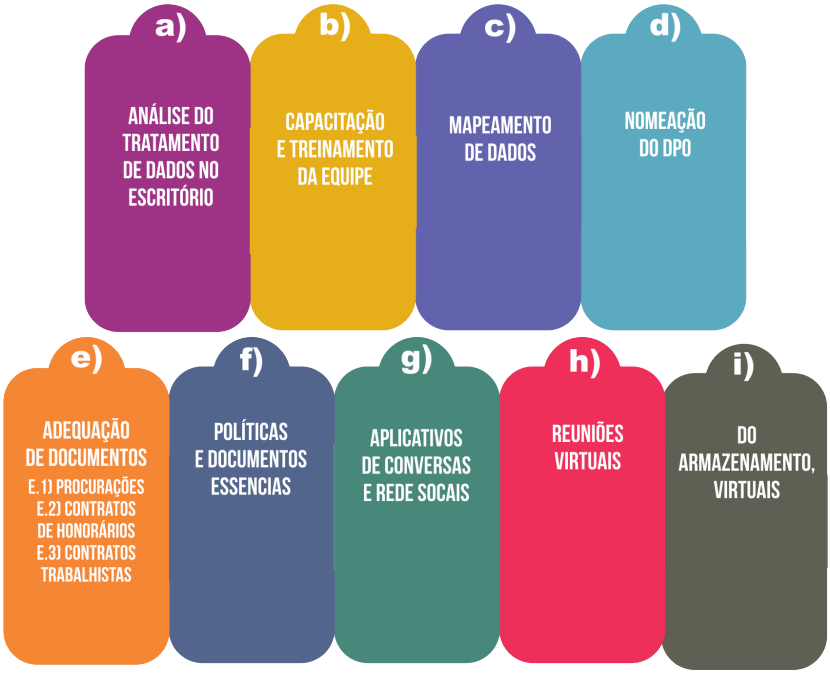
A Lei trouxe importantes direitos que o titular pode exercer perante qualquer instituição pública ou privada que faça uso de seus dados pessoais, como nome, dados cadastrais e outros.

O titular dos dados pessoais tem o direito de requisitar das empresas e instituições, a qualquer momento:
I. a confirmação da existência de tratamento;
II. o acesso aos dados mantidos pelo controlador;
III. a correção de dados incompletos, inexatos ou desatualizados;
IV. a anonimização, bloqueio ou eliminação de dados, desde que sejam considerados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
V. a portabilidade de seus dados pessoais a outro fornecedor de serviço;
VI. a eliminação dos dados pessoais quando retirado o consentimento dado anteriormente;
VII. a relação de com quem seus dados foram compartilhados;
VIII. a informação de que poderá negar consentimento e quais suas consequências;
IX. a revogação do consentimento.

Ainda assiste à pessoa física o direito de peticionar contra os agentes de tratamento diretamente à Autoridade Nacional de Proteção de Dados, que exerce fiscalização e controle sobre aqueles (artigo 18, §1º).

Quando uma decisão a respeito de seus dados pessoais é tomada com base em tratamento automatizado, o titular tem direito à revisão dessa decisão (artigo 20). O exercício dos direitos decorrentes da proteção de dados pode ser feito individualmente pelo titular ou por tutela coletiva, quando procurados os órgãos do sistema de Justiça que desempenham essa função (ex.: Defensoria Pública, Ministério Público, Idec, Procon e OAB).

MEDIDAS QUE DEVEM SER ADOTADAS



5. MEDIDAS QUE DEVEM SER ADOTADAS

a) Análise do tratamento de dados pessoais no escritório

Por Carlos Henrique Garcia de Medeiros

A Lei nº 13.709/18 traz vinte verbos em seu Art. 5º, inciso X, dentre as quais incluem-se as atividades de coleta, utilização, acesso, reprodução, arquivamento, armazenamento e eliminação, não se limitando a estas.

Das operações de tratamento decorrem dez hipóteses que legitimam e permitem a realização das atividades acima elencadas, ao que se convencionou rotular como bases legais, explicitadas nos incisos do Art. 7º do referido texto legal, sem grau de hierarquia ou dependência entre elas

Logo em seu primeiro inciso, o Art. 7º nos apresenta a primeira das bases legais: o consentimento do titular de dados, que é a manifestação livre, informada e de forma inequívoca pela qual o titular aceita o tratamento de seus dados pessoais com finalidade especificada.

Merece destaque, ainda, a hipótese na qual o tratamento de dados for necessário para a execução de contrato ou procedimentos preliminares a este relacionados (Art. 7º, V), como é o caso da coleta de dados pessoais para confecção de contrato imobiliário ou de compra e venda entre partes, para citar alguns exemplos.

Quando o cliente conosco contrata honorários advocatícios, e em seguida assina instrumento procuratório e demais documentos pertinentes, para posterior propositura de uma ação judicial ou realizar tratativas de seus interesses, enquanto advogados estamos legitimados a utilizar aqueles dados ali dispostos com base no Art. 7º VI, que elucida ser possível o tratamento de dados para exercício regular de direitos em processo judicial, administrativo ou arbitral.

O cliente deve ser informado destes procedimentos de tratamento de dados, e o ideal é que tome conhecimento antes do início da prestação dos serviços jurídicos, através de cláusula destacada em contrato de honorários, com redação clara e específica, informando quais dados serão utilizados, com quais instituições haverá o compartilhamento destes e por qual modo e quanto tempo serão estes armazenados.

Por óbvio, o processo de adequação à Lei Geral de Proteção de Dados de um escritório de advocacia não pode se limitar aos dados pessoais de novos clientes. A revisão de contratos de honorários vigentes também se mostra essencial, e pode ser feita através de termos aditivos de contrato.

Outro ponto que merece destaque: Tenha cautela com os parceiros e prestadores de serviço de seu escritório. Infelizmente, nem todos os parceiros estão sensibilizados para as adequações necessárias. Em certos cenários, caso uma destas empresas sofra com incidentes de segurança, os danos decorridos desta falha podem respingar na sociedade advocatícia. Seria o caso, por exemplo, de profissional parceiro em determinada área que deixa que informações confidenciais de determinado cliente saiam de sua esfera de controle.

Jamais se esqueça que a LGPD é um trabalho conjunto. De nada adianta se sua casa está organizada e devidamente adequada se seu vizinho, com quem mantêm-se laços de parceria ou interdependência, mostra-se frágil quanto a questões de segurança e alheio à necessidade de adequação.

b) Capacitação e treinamento da equipe

Por Kellyne Laís Laburú Alencar de Almeida

Inúmeras são as tarefas de que o agente de tratamento deve se desincumbir para manter seguros os dados pessoais e, no mais das vezes, os esforços são especialmente direcionados à obtenção de recursos tecnológicos e à produção e adequação de documentos.

A capacitação e o Treinamento da equipe são fundamentais e não podem ser negligenciados, sob pena de se tornarem o calcanhar de Aquiles do projeto de implementação do Programa de Privacidade e Proteção de Dados Pessoais: estudos demonstram que cerca de um terço dos incidentes com dados pessoais são resultado de falha humana decorrente de inadequado treinamento de pessoal[10] , o que pode gerar danos relevantes às finanças, marca, posição de mercado e imagem da empresa responsável.

Assim, se é verdade que o processo de implementação naturalmente implica a contratação e uso de re-

10. Dados do estudo "Custos de Violação de Dados 2017", realizado pela IBM em parceria com o Instituto Ponemon.

cursos tecnológicos disponíveis, o desenvolvimento de políticas corporativas e a adequação de documentos e contratos, os esforços não podem se restringir apenas a eles: a verdadeira adequação passa necessariamente por uma profunda e completa mudança de cultura organizacional direcionada à proteção de dados pessoais e ao desenvolvimento de um modelo de gestão que analise os riscos da atividade desenvolvida e busque sua eliminação ou – ao menos – mitigação. Muito além de instrumentos ou documentos, a aplicação real dos preceitos da LGPD ao dia a dia do negócio passa pela educação das pessoas que coletam e tratam os dados pessoais.

A capacitação da equipe deve ter início com a apresentação dos principais preceitos da LGPD e a conscientização sobre a importância da proteção dos dados pessoais a fim de garantir, ao titular, o exercício dos direitos à liberdade, à privacidade e ao livre desenvolvimento da personalidade, e, ao negócio, a valorização de sua imagem e a mitigação dos riscos de sanções.

É importante ainda destacar que esse processo deve se iniciar pela alta administração e seguir em direção aos colaboradores de todos os cargos e funções, pois a abordagem *top-down* costuma ser mais eficiente na

conscientização sobre a necessidade de respeito e aplicação do novo modelo de gestão a ser desenvolvido.

Nesse sentido, uma proposta interessante é a realização de uma oficina – presencial ou *on-line* – iniciada com a apresentação do objeto, conceitos e principiologia da LGPD (art. 1º a 6º), explanação das bases legais e suas peculiaridades (art. 7º e 11), definição dos agentes de tratamento de dados (art. 37 a 41) e das suas respectivas responsabilidades (art. 42 a 45), garantindo-se ainda espaço para comentários e dúvidas dos participantes.

Outra medida interessante é o envolvimento de toda a equipe ao longo do processo de implementação do Programa de Privacidade e Proteção de Dados Pessoais, pois a participação direta dos envolvidos proporciona a explanação prática do fluxo dos dados pessoais, dos riscos do negócio e dos deveres e procedimentos que incumbem a cada área para que a adequação seja real. Dessa forma, torna-se possível a construção de conhecimento alinhado com as características específicas do negócio, preparando os colaboradores para resolver as questões que efetivamente farão parte de suas atividades diárias.

Ponto importante, ainda relacionado a capacitação e treinamento, é a criação de código de conduta direcionado à equipe do qual constem as obrigações legais e contratuais dos diversos envolvidos no tratamento dos dados pessoais. Nesse caso, a consideração da própria estrutura, bem como da escala, volume e sensibilidade dos dados tratados, é fundamental para compreensão do nível de detalhamento e desenvolvimento desses documentos internos que norteiam a equipe em suas diversas atividades. Para escritórios maiores, com intenso fluxo de dados pessoais interna e externamente, a criação de políticas corporativas e códigos de conduta específicos para cada departamento passa a ser essencial na demonstração do comprometimento com as boas práticas relativas à proteção de dados pessoais.

A preocupação com a conscientização e capacitação da equipe interna deve ser ainda estendida a terceiros, fornecedores de serviços e parceiros, que atuem junto ao negócio na posição de operadores de dados ou de controladores conjuntos. Afinal, a LGPD estabelece a responsabilidade solidária em caso de tratamento conjunto de dados pessoais, motivo pelo qual as equipes de todos os envolvidos devem estar em sintonia de atuação.

Por fim, é preciso compreender que o trabalho de treinamento da equipe não se encerra com a tomada das medidas sugeridas acima, devendo manter-se cíclico e contínuo para que seja eficiente. A mudança da cultura organizacional e o desenvolvimento do modelo de gestão de privacidade e proteção de dados pessoais levam tempo e exigem paciência e investimento de todos os envolvidos. Assim, a definição de um cronograma de atividades que mantenha a equipe bem informada e comprometida com o cumprimento de seus deveres é essencial para a efetiva e almejada proteção dos dados pessoais.

c) Mapeamento de dados

Por Fernando Henrique Baena Alli

O mapeamento de dados é uma das fases mais importantes em um processo de adequação à LGPD. É nesse momento que todas as operações de tratamento de dados são mapeadas, assim, avalia-se o ciclo de vida do dado pessoal desde a sua coleta ou produção, passando pelo compartilhamento, arquivamento, reprodução até a exclusão ou anonimização. Importante ressaltar que a LGPD traz vinte verbos que definem o tratamen-

to de dados e que esses verbos fazem remetem ao ciclo de vida do dado pessoal.

A Lei Geral de Proteção de Dados em seu art. 37 estabelece que "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".

É nesse sentido que se aplica o mapeamento de dados, além de ser um importante passo para entender o processamento de dados dentro da organização, como consequência, também é relevante para manter os registros das operações de tratamento de dados pessoais conforme visto no art. 37 da LGPD. Assim, é possível entender os procedimentos e o caminho que os dados percorrem.

Dessa forma, quando realizamos um mapeamento de dados analisamos as operações de processamento de dados, definindo quais são os dados coletados, qual a finalidade do tratamento, ajustando a operação às bases legais, tempo de retenção e local onde aqueles dados estão armazenados.

Para realizar o mapeamento de dados, existem algumas técnicas que auxiliam nesse procedimento, a título de exemplo podemos citar o questionário e as entrevistas.

Em seguida ao levantamento das operações de tratamento de dados pessoais e realização do mapeamento de dados, será realizada a análise de riscos. Assim, observa-se além das recomendações legais outras normas como ISO 27001, a qual trata da segurança da informação.

Avalia-se, então, as medidas físicas, técnicas e organizacionais adotadas para garantir a segurança dos dados pessoais, bem como sua confidencialidade, integridade e disponibilidade.

Ao final da análise de riscos, faz-se uma matriz de riscos elencando os riscos pelas variáveis (probabilidade/consequência).

Portanto, o mapeamento de dados é o coração da implementação, uma vez que quanto mais detalhado e minucioso for, mais fácil será executar as próximas etapas.

d) Nomeação do DPO

Por Maria Gabriela Lordelo de Vasconcelos

Conforme descrito no tópico 3, item g, Encarregado pela Proteção de Dados Pessoais é a 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).

A legislação prevê, de forma ampla, em seu artigo 41, que o controlador deverá indicar encarregado pelo tratamento de dados pessoais. Da leitura do dispositivo devemos assumir que toda organização que se enquadre nas hipóteses de incidência da LGPD deve nomear uma pessoa para este papel.

Entretanto, o parágrafo 3º do artigo 41, estipula que a ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação.

Neste sentido, o Conselho Diretor da ANPD aprovou o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte (Resolução CD/ANPD

n. 02/2022). São considerados ‘agentes de pequeno porte’ microempresas e empresas de pequeno porte, bem como pessoas naturais que realizam tratamento de dados pessoais, assumindo as obrigações típicas de controlador ou de operador.

Para fins de aplicação aos escritórios de advocacia, devemos considerar a forma pela qual o escritório está constituído ou se o advogado atua de forma autônoma, sem constituição de entidade jurídica, ou seja, como pessoa natural.

Considerando que os escritórios podem ser constituídos por meio de sociedades simples ou sociedades limitadas unipessoal, a resolução supramencionada deve ser observada.

O artigo 11 da Resolução estabelece a dispensa de indicação do encarregado pelos agentes de tratamento de pequeno porte.

Não obstante a desobrigação, o escritório/advogado deverá disponibilizar um canal de comunicação com o titular de dados, para comunicar-se com o mesmo, aceitar reclamações, prestar esclarecimentos e adotar providências.

Por fim, vale ressaltar que a indicação de um Encarregado será considerada como uma boa prática e medida de governança a ser observada para a dosimetria de uma eventual sanção.

Caso o escritório opte por nomear um Encarregado, a LGPD não estipula um perfil específico para o posto, podendo ser pessoa física ou jurídica, membro do escritório ou um agente externo. É recomendável, no entanto, que a nomeação seja feita por um ato formal: um ato administrativo ou um contrato de prestação de serviços, respectivamente.

A Autoridade Nacional de Proteção de dados prevê na sua agenda regulatória 2021-2022 a elaboração da Norma do Encarregado, que deverá indicar características e atribuições, formas de atuação do Encarregado, terceirização e responsabilização, informação de contato do Encarregado, dispensa e flexibilização de indicação, dentre outros. Até a data da publicação do presente manual a norma não havia sido publicada.

Enquanto isso, nos baseamos nas diretrizes internacionais. O article 29 Data Protection Working Party foca a orientação de escolha do Encarregado sobretudo no

seu conhecimento especializado das normas e práticas de proteção de dados, que deve ser proporcional e adequado à criticidade dos dados tratados e da segurança necessária.

e) A adequação de documentos
e.1) Procurações

Por Maíra Salgueiro Freire

A adequação à Lei Geral de Proteção de Dados – LGPD em um escritório de advocacia, exige a adequação de documentos imprescindíveis para o exercício jurídico da nossa profissão em uma demanda judicial, sendo eles: procuração e contrato de honorários.

Note-se que é admitido expressamente pela LGPD o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral, ao passo que a lei consagra o princípio da finalidade segundo o qual pressupõe-se *"a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".*

Entretanto, a lei não apresenta remissão de autorização para manutenção desses dados nos sistemas informatizados utilizados pelos escritórios de advocacia ou a utilização desses dados de forma extrajudicial, como a atuação de forma consultiva.

Dessa forma, por prudência, o advogado pode resguardar a lisura no tratamento de dados de seus clientes constando cláusula expressa de consentimento de utilização dos dados digitais pelo titular, cuja finalidade deve recair exclusivamente para o exercício de direitos em processos judiciais e/ou administrativos.

Quanto especificamente a procuração, é importante se atentar na elaboração do documento para a coleta dos dados somente necessários à confecção e validação da outorga de poderes, com a inclusão da base legal de tratamento, nos termos do artigo 7º da Lei 13.709/2018.

Como exemplo, a seguinte redação:
“Considerando a Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), nos termos do artigo 7º, (a) OUTORGANTE declara ter ciência da necessidade dos dados aqui coletados e dá consentimento do uso dos seus dados pelos OUTORGADOS para a finalidade

exclusiva de (solução jurídica aqui pretendida), em observância ao cumprimento das regras quanto a proteção de dados, diante dos princípios da necessidade, finalidade e/ou autodeterminação informativa, inclusive no tratamento de dados pessoais sensíveis, de acordo obrigação legal de coleta dos dados."

e.2) Contratos de honorários:

Por Maíra Salgueiro Freire

Como ressaltado, é imprescindível a adequação às normas da LGPD também nos contratos de honorários com a revisão dos contratos existentes, não se limitando aos contratos de honorários, incluindo também aqueles com parceiros e fornecedores externos e a elaboração de novos modelos já em consonância com a Lei.

Portanto, temos aqui a análise de duas situações específicas:
1) Contratos vigentes: elaboração de um termo aditivo de contrato ou termo de consentimento (se for o caso).
2) Novos contratos: inserir cláusulas de proteção de dados específicas e de acordo com o mapeamento de dados do seu escritório.

Para a confecção dessas cláusulas no contrato em adequação à LGPD deve verificar como funciona o fluxo de dados no seu escritório, quais tipos de dados são coletados, onde são armazenados, com quem é compartilhado e como são descartados.
Assim, cumpre pontuar algumas possíveis cláusulas para inclusão no seu contrato de honorários:
1) cláusula conceitual LGPD;
2) cláusula do tipo de dados pessoais e dados pessoais sensíveis;
3) cláusula sobre a atuação do escritório como controlador;
4) cláusula específica de tratamento de dados;
5) cláusula de compartilhamento;
6) cláusula de transferência de dados;
7) cláusula de armazenamento;
8) cláusula de direito dos titulares;
9) cláusula de incidente de segurança
10) cláusula de canal de comunicação

e.3) Contratos trabalhistas

Por José Francisco de Souza Bezerra Carvalho

Não há dúvidas que a LGPD se aplica aos contratos de trabalho. Isso se torna claro pelo fato da norma possuir

um artigo destinado às exceções de sua aplicação e por ele não fazer qualquer menção aos vínculos trabalhistas (vide art. 4º da LGPD).

Quanto aos escritórios de advocacia, esses podem trabalhar com diferentes regimes de colaboração, sejam vínculos de emprego, de prestação de serviço, associação ou outros tipos.

O cuidado com o tratamento de dados pessoais não é uma novidade para o setor responsável pela gestão de recursos humanos, pois existe uma ampla gama de leis e regulamentações trabalhistas que, por si só, já determinavam obrigações que implicam uso de dados pessoais ou, no dizer da nova Lei, implicam tratamento de dados pessoais.

De modo geral, a recomendação dada consiste em sempre realizar o tratamento de acordo com a lei ou regulamentação aplicável. Isso porque a própria LGPD estipula que o tratamento de dados pessoais é autorizado quando feito para cumprir com obrigação legal ou regulamentar existente (Art. 7, II, da LGPD).

No que toca aos contratos de trabalho, a partir do momento em que o colaborador é aprovado no processo

seletivo podem ser coletados, para fins de exemplificação, os seguintes dados pessoais: Nome; RG; CPF; Dados bancários para fins de pagamento; Endereço; Número de PIS/ PASEP/ NIS; Carteira de Trabalho e Foto.

A coleta dos dados supracitados encontra respaldo, em um primeiro momento, na base legal da execução do contrato. Segundo esta base, podem ser tratados dados pessoais quando a finalidade for a de permitir a execução de um contrato no qual o titular de dados possui interesse na execução (artigo 7, V da LGPD).

Além dos dados citados acima, há uma série de outros documentos que podem ser solicitados, conforme a posição do colaborador, nos quais constam diversos dados pessoais.

Novamente ressalta-se que nenhum dado pessoal pode ser exigido caso este não esteja atrelado à função a ser exercida pelo colaborador, sendo ele estritamente necessário para a elaboração do contrato/vínculo formal a ser estabelecido entre o escritório de advocacia e o colaborador.

Vale aqui mencionar a exigência, para fins de contratação regidas pela CLT, a realização de um exame médico admissional. Mesmo sendo produzido um dado de

saúde e, portanto, um dado sensível, este não necessita de qualquer consentimento adicional, tendo em vista o amparo legal para sua coleta.

Cabe também aqui mencionar os dados utilizados para a inclusão no sistema E-Social. Sendo um sistema informatizado da administração pública, cujo abastecimento com informações trabalhistas, fiscais e previdenciárias é obrigatório, o registro de dados pessoais de empregados feito pelo escritório de advocacia em tal sistema está coberto pela base legal do cumprimento de obrigação regulatória (Art. 7, II, LGPD).

Nos casos em que a CLT ou outra fonte regulatória de direito solicitar que, para a realização de um vínculo de um colaborador seja fornecido algum dado sensível, tal requisição estará respaldada pela base da obrigação legal (artigo 7, II da LGPD) e, portanto, poderá ser fornecida sem qualquer requisito adicional.

Por fim, recomenda-se:
a) inserir cláusula contratual nos contratos de trabalho ou celebrar aditivo contratual a fim de informar ao empregado como será realizado o tratamento de seus dados dentro da empresa;

b) elaborar um termo de tratamento de dados pessoais para aqueles colaboradores que não possuem contrato formal, a fim de informar ao titular como será realizado o tratamento de seus dados dentro da empresa;
c) elaborar um termo aditivo ao contrato de trabalho do colaborador escolhido para atuar como DPO, a fim de delimitar suas responsabilidades e obrigações.

f) Políticas e documentos essenciais

Por Fernando Henrique Baena Alli

As políticas e documentos têm como objetivo demonstrar à ANPD que o escritório passou pelo processo de adequação à LGPD. Por isso, todo o processo deverá ser documentado. Sendo assim, uma boa política reflete os objetivos de uma organização e direciona as suas ações; portanto, essas condições são realmente sintomas de boas práticas.

Políticas devem:

- Ser capazes de ser implementadas;
- Ser executáveis;
- Ser concisas e fáceis de entender; e
- Ter equilíbrio entre proteção e produtividade;

Política precisam:

- Explicar a necessidade da política;
- Descrever o que é coberto pela política;
- Definir contatos e responsabilidades;
- Incluir pelo menos um objetivo;
- Explicar como as violações serão tratadas

O processo de adequação à LGPD é repleto de políticas e documentos, nem todos os documentos constantes aqui serão aplicáveis a todos os tipos de escritórios, haja vista que isso dependerá do mapeamento de dados e consideração das particularidades de cada escritório.

Documentos :

1. Política de Privacidade;
2. Termos e Condições de Uso;
3. Termo de Nomeação da Comitê;
4. Termo de Nomeação do DPO;
5. Atas do Comitê;
6. Política de Cookies;
7. Aditivos de Contratos;
8. Norma de Gestão de Incidentes;
9. Procedimento de Demanda de Titulares;
10. Termo de Consentimento;
11. Termo de Revogação do Consentimento;

12. Política de Uso de Dispositivos Móveis;
13. Política de Retenção;
14. Mapeamento de dados
15.Aviso de Privacidade
16. Relatórios de Impacto na Proteção de Dados
17. Relatório de Assunção de Riscos

No entanto, existem alguns documentos que podem aplicáveis a quase todos ou a maioria dos escritórios:

1. Política de privacidade
Uma política de privacidade disponível para o público deve ser uma consideração primária para assegurar que o tratamento respeita os princípios da LGPD.
A sua política de privacidade deve estar prontamente acessível no mesmo local em que você coleta dados pessoais. Se os dados são coletados via website, a política deve estar disponível lá.

2. Norma de gestão de incidentes
De acordo com a ANPD:
INCIDENTE: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mu-

dança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

INCIDENTE DE SEGURANÇA: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores (ANPD, 2021. Pág. 9).

Dessa forma, um incidente de segurança com dados pessoais é qualquer evento adverso CONFIRMADO que tenha relação com violação na segurança de dados pessoais, por exemplo, acesso não autorizado, evento ilícito ou acidental que resulta na destruição, perda, alteração, vazamento ou qualquer tratamento de dados inadequado.

Conforme a LGPD, cabe ao controlador comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos relevantes. Cabe à ANPD a regulamentação das situações de risco ou dano relevante ao titular. Até o momento

da publicação deste guia, a ANPD ainda não havia regulamentado o tema, mas se recomenda que os leitores acompanhem continuamente o site e os demais canais oficiais da Autoridade para novidades e atualizações.

Paralelamente, a organização deverá avaliar o risco no âmbito interno, com objetivo de estipular se há ou não risco ou dano relevante para a comunicação do incidente ao titular. Nesse sentido, a ANPD disponibiliza que no âmbito interno da organização devem ser levadas em consideração os seguintes itens:
a. Qual vulnerabilidade foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.
b. Fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.
c. Categoria de dados pessoais: dados sensíveis, dados pessoais de crianças e adolescentes.
d. Extensão do vazamento: quantificar os titulares e os

dados pessoais que tiveram a sua segurança violada neste evento.
e. Avaliação do impacto ao titular: avaliar quais são os impactos que o incidente pode gerar aos titulares.
f. Avaliação do impacto no serviço: avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

3. Política de cookies

A política de Cookies do Google define que um cookie é um pequeno texto enviado ao navegador pelo site que você visita. Com ele, o site lembra das informações sobre a visita, o que facilita seu próximo acesso e deixa o site mais útil para você.

Por exemplo, cookies são usados para lembrar seu idioma preferido, mostrar anúncios mais relevantes para você, contar quantos visitantes os proprietários de uma página recebem, além de ajudar os visitantes a se inscreverem nos serviços, proteger seus dados e lembrar suas configurações de anúncios.

É muito comum em sites que as políticas de cookies se resumem a aceitar ou não aceitar os cookies sem nenhum nível de personalização, no entanto, a LGPD permite que o titular saiba quais são os cookies e quais as consequências de não os aceitar.

g) Aplicativos de conversa e redes sociais

Por Jaqueline Nais Inoue e Giuliana Gattass

O uso das redes sociais e aplicativos de conversa se tornou um hábito cada vez mais frequente nesse novo normal, inclusive no exercício da profissão pelos advogados.

Os advogados utilizam-se diariamente um grande volume de dados pessoais, de clientes, colaboradores e prestadores de serviços e partilham muitos documentos com colegas do mesmo escritório ou de escritórios parceiros e tribunais nos aplicativos e as vezes até nas redes sociais. onde os documentos digitalizados substituíram em grande parte os documentos físicos.

Tal substituição ocorreu por facilitar à capacidade de visualização dos documentos de modo mais célere e facilita também o compartilhamento tanto de docu-

mentos como de dados pessoais, via dispositivos (celular, *tablet*, computador ou notebook).

Algumas atitudes que os advogados e os escritórios precisam adotar para se protegerem

1. Ter regras claras no Código de Conduta e em Políticas internas sobre o uso da internet, intranet, celular corporativo, e-mail, aplicativos de conversa e redes sociais;
2. Ter criptografia de ponta a ponta;
3. Ter regras claras sobre a partilha de imagem e áudio no escritório;
4. Definir inclusive as sanções que podem ocorrer no caso de descumprimento das regras;
5. Criar também uma Política de Backup e de Retenção de Documentos;
6. Manter sempre cópia de segurança dos dados pessoais tratados pelo escritório, se possível uma copia física e uma digital;
7. Trocar senhas periodicamente e usar senhas mais complexas nos dispositivos que utilizar no escritório (comprimento considerável, usando-se letras maiúsculas e minúsculas, números e símbolos);
8. Observar sempre a finalidade de uso informada na solicitação dos dados;
9. Não salvar dados do cartão de crédito do escritório

quando fizer operações online;
10. Conferir a procedência de links e páginas antes de acessar;
11. Verificar todas as Política de Cookies, Política de Privacidade e Termos de Uso;
12. Observar a configuração de privacidade de dados cadastrais (quem pode visualizar, localizar em buscadores e compartilhar);
13. Observar a configuração de privacidade ou situações de exposição da intimidade que facilite a obtenção de dados pessoais (informação relacionada à pessoa natural identificada ou identificável – ex.: filiação, telefone, endereço, e-mail, etc.);
14. Ter cuidado com os dados tornados manifestamente públicos publicados em redes sociais (hipótese em que o consentimento do titular não será solicitado, ainda que o tratamento dos dados observe a LGPD);
15. Observar uso indevido (não consentido) de tecnologia de reconhecimento facial;
16. Atenção à solicitação de coleta de impressões digitais por aplicativos;
17. Observar o uso de algoritmos (preferências individuais) para fins de publicidade e compartilhamento com terceiros;
18. Questionar as empresas se houver algum tipo de sus-

peita de discriminação no mercado de consumo, como preços diferenciados de produtos ou serviços ofertados;
19. Observar em quais aplicativos ou redes sociais, usados eventualmente ou habitualmente, há compartilhamento de geolocalização e a periodicidade (pontual ou contínua);
20. Observar se o aplicativo ou a rede social oferece meio claro e de fácil utilização para solicitar informações sobre o tratamento dos dados pessoais ou para revogação do consentimento.

h) Reuniões virtuais

Por Giuliana Gattass

As reuniões virtuais tornaram-se frequentes nos últimos anos, através de diversas plataformas diferentes. Em todas as reuniões é sempre fundamental estar atento as regras da LGPD no tocante a Proteção de Dados e Segurança da Informação.

Algumas atitudes que os advogados e os escritórios precisam adotar nas reuniões virtuais
1. Somente grave a reunião depois que todos participantes consentirem expressamente a gravação;
2. Verifique os dados que fazem parte do material que

será compartilhado com antecedência
3. Somente compartilhe dados, dados sensíveis e dados de crianças e adolescentes que sejam fundamentais serem partilhados
4. Mantenha sempre o antivírus atualizado.
5. Crie senhas e links específicos para acesso, para anfitrião e convidados, como por exemplo;
6. Tenha atenção e evite autorizar o acesso a desconhecidos, que podem ter sido inseridos por malwares.

i) Do armazenamento, retenção a exclusão dos dados

Por Carlos Henrique Garcia

Culturalmente os escritórios de advocacia são acumuladores de dados, mantendo documentos desnecessários por décadas – muitas vezes originais – relativos a demandas judiciais que se findaram há muito tempo.

Este comportamento não é visto com bons olhos pelas disposições da Lei Geral de Proteção de Dados.

Elaborar o mapeamento de fluxo de dados e compreender cada etapa deste ciclo se mostra imprescindível para alcançar a conformidade com a Lei Geral de

Proteção de Dados, demonstrando eticidade e transparência ao titular de dados.

A partir do momento em que novas informações de titulares de dados entram nos arquivos físicos e sistemas computacionais do escritório de advocacia, um ciclo de vida dos dados se inicia, justamente com a coleta, passando ao seu processamento, análise, utilização e compartilhamento, arquivamento e, ao final, com a sua exclusão.

Desde a recepção dos dados pessoais a ponderação deve se fazer presente. É preciso que haja a minimização de dados, com a coleta daqueles estritamente necessários para a finalidade a qual se destinam, respeitando-se os princípios da boa-fé, necessidade, finalidade e outras bases legais dispostas no Art. 6º da LGPD.

Passo seguinte à coleta, os dados pessoais serão analisados – se se relacionam com o objeto da demanda judicial – armazenados – seja em meio físico ou digital – para sua posterior utilização.

Durante o armazenamento das informações, recomenda-se que o escritório de advocacia organize seu acervo de dados com base em hierarquia e níveis de aces-

so, de modo que advogados de determinada área de atuação possam acessar somente as informações dos clientes pelos quais são responsáveis. Limitar o poder de modificação, alteração e/ou exclusão de dados aos sócios do escritório também mostra adequado.
Quanto à guarda de documentos físicos, garanta que os mesmos estejam armazenados em local seguro, livre de umidade, pragas ou incidência de luz solar direta, fatores que podem deteriorar sua integridade. Sempre que necessário utilize chaves e/ou cadeados para controle de acesso.

Atente-se ao fato de que, se o titular de dados se valer de seu direito de revogação do consentimento ou oposição ao tratamento de dados, a retenção de documentos deve cessar.

Do armazenamento decorre outro importante tópico: A retenção dos documentos. Afinal, por quanto tempo devo manter os documentos dos meus clientes e colaboradores dentro dos sistemas e arquivos do meu escritório?

Aqui precisamos levar em conta a necessidade da continuidade de tratamento de dados para atender disposições de obrigações legais ou regulatórias e atendi-

mento aos interesses legítimos do controlador ou de terceiros (Art. 7º, II e IX, LGPD).

Veja, a seguir, importantes informações a este respeito:
• Em relação a fornecedores e prestadores de serviços, recomenda-se que se retenha os documentos pelo prazo contido nos artigos 205 e 206 do Código Civil combinado com o Código de Defesa do Consumidor.
• **Área Penal**: Mantenha consigo os documentos com base no tempo da prescrição calculada com base na pena de um crime.
• **Área Trabalhista:** Documentos inerentes a colaboradores e prestadores de serviços devem ser guardados por dois anos a contar do fim do contrato de trabalho; Depósitos do FGTS por 30 anos e contribuições previdenciárias por 10 anos.
• **Área Civil**: Observe o disposto nos artigos 205 e 206 do Código Civil, e a natureza do objeto da ação.
• **Área Tributária**: Em regra 5 (cinco) anos, contados da constituição do débito, de acordo com Art. 173, I.
• **Área Previdenciária**: Os documentos devem ser guardados pelo prazo de 10 (dez) anos, aplicando-se à folha de pagamento, ao recibo e ficha de salário-família, aos atestados médicos relativos a afastamentos e incapacidade ou à guia de recolhimento de contribuição previdenciária.

Por fim, abordando a etapa derradeira do ciclo de vida dos dados, no processo de eliminação deve se alcançar a completa destruição das informações contidas no documento.

Apesar de tratar a eliminação como etapa importante, a LGPD é vaga no que diz respeito às formas ou recomendações como isso deve ser feito. Espera-se que a Agência Nacional de Proteção de Dados – ANPD – complemente essa lacuna através de materiais educacionais e orientações.

Entretanto, algumas diretrizes de boas práticas podem ser utilizadas pelos escritórios. A exemplo de cópias de documentos físicos, que podem ser inutilizados, com o uso de máquinas fragmentadoras de papéis, ou mesmo incinerados.

Já no que diz respeito aos documentos digitais/digitalizados, a forma adequada de eliminá-los é através de sobrescrição de dados no hardware, no local onde a informação original estava alocada. Técnicas como essa podem ser implementadas facilmente através de programas computacionais, como o Basefy, por exemplo.
Uma equipe competente de tecnologia da informação

– interna ou parceira – também pode lhe auxiliar na aplicação de meios de anonimização de dados, garantindo que, caso um terceiro estranho à sua organização tenha acesso ao banco de dados não consiga interpretar as informações ali contidas.

Havendo a necessidade de descarte de mídias físicas (CD'S, DVD's, Disquetes e Pen Drives), ou componentes computacionais (HD'S e SSD's) busque formatá-los e destruí-los completamente.

6. DA RESPONSABILIDADE PELO TRATAMENTO DE DADOS PESSOAIS E SANÇÕES ADMINISTRATIVAS

Por Diogo Ferreira Rodrigues

A responsabilidade do agente de tratamento de dados, no caso o advogado ou o escritório de advogados, é disciplinada nos artigos 42 a 45 da Lei 13.709/18 (LGPD) estabelecendo, logo de início (Art. 42), que o controlador ou operador de dados pessoais que causar dano a outrem é obrigado a repara-lo.

O legislador preocupou-se ainda em assegurar a possibilidade de inversão do ônus da prova em favor do titular dos dados, nos casos em que verificar ser verossimilhante a alegação, houver hipossuficiência para fins de produção da prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa (§2º, art. 42).

Percebe-se, portanto, que a lei buscou trazer de forma expressa e muito clara o dever de reparação dos danos

causados no exercício da atividade de tratamento de danos pessoais, possibilitando, inclusive, a inversão do ônus da prova em favor do titular dos dados, cujo tratamento teria dado origem ao dano alegado.

Assim, é muito importante para o exercício da atividade de tratamento de dados pessoais a observância ao disposto no art. 6º da LGPD, que estabelece os 10 princípios norteadores da atividade de tratamento, sendo eles: Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Responsabilização e Prestação de contas.

Nota-se que a responsabilidade é tratada como um dos princípios legalmente estabelecidos para a prática da atividade de tratamento de dados juntamente com a boa-fé. Outro ponto que merece atenção é o atendimento aos requisitos para o tratamento de dados pessoais (art. 7º e seguintes), que deve ser preenchido para o regular exercício da atividade. Portanto, existindo alegação por parte do titular, da ocorrência do dano patrimonial, moral, individual ou coletivo; ao agente de tratamento incumbirá a prova da ocorrência das excludentes do art. 43 (não realizou o tratamento; realizou sem violação

a legislação ou a culpa exclusiva do titular dos dados), para afastar o dever de reparação.

A obediência ao disposto no artigo 43 por parte do agente, é de extrema importância, tendo em vista a possibilidade de inversão do ônus da prova prevista no §2º do art. 42, nos casos de alegação de danos sofridos pelo titular, pois só assim será capaz de evitar a sua responsabilização. As excludentes previstas nos incisos I e III do aludido art. 43, dizem respeito às situações em que o agente não realizou o tratamento (inciso I); ou que o dano é decorrente de culpa do titular ou de terceiro (inciso III). Já o inciso, II, do art.43, exige a demonstração por parte do agente de que não houve qualquer violação a legislação de proteção de dados durante o tratamento dos dados que resultaram no dano alegado. Para a obtenção da excludente de responsabilidade invocada em prestigio ao disposto no aludido dispositivo legal, fazer-se mister que agente de tratamento tenha observado todas as exigências legais para a pratica do ato, mormente o respeito aos princípios e requisitos para o tratamento.

Medidas como a implementação de boas práticas de Governança através de um departamento de Com-

pliance (artº 50), bem como de medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados (art. 46), mostram-se bastante relevantes na medida que podem influenciar no resultado reduzindo o patamar de aplicação de sanções administrativas (art. 52§1º).

Como dito, os Agentes de Tratamento de Dados, além da responsabilidade civil, estão sujeitos as sanções administrativas pelo tratamento irregular, aplicáveis pela ANPD, que correspondem ao art. 52, consubstanciando-se em: 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.

Após o procedimento administrativo que possibilite aos agentes a oportunidade de contraditório e ampla defesa, sendo confirmado o desrespeito ou a infração das regras da LGPD, poderão ser aplicadas sanções administrativas, de forma gradativa, isolada ou cumulativamente.

Os critérios e parâmetros para a aplicação das sanções estão previstos no art. 52, § 1º: 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; 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.

Importante registrar ainda, que a responsabilização administrativa prevista na LGPD, não afasta a aplicação das regras de responsabilidade previstas no Código Civil (arts. 186, 187 e 927) e no Código de Defesa do Consumidor.

Em síntese ao Agente de Tratamento de Dados Pessoais impõe-se a estrita obediência aos princípios e demais requisitos legais para o tratamento de dados estabelecidos na LGPD sob pena de responsabilidade ; enquanto ao Titular dos Dados, resta assegurado, por consequência lógica, o direito a reparação de todos os danos sofridos, contanto ainda com a possibilidade de inversão do ônus da prova a seu favor.

7. CONSIDERAÇÕES FINAIS

Por Giuliana Gattass

Na rotina dos escritórios de advogados é obrigatório adotar o sigilo profissional durante todo o período do tratamento de dados.

A promulgação da LGPD trouxe novas regras que devem ser implementadas tanto em empresas, como e associações, fundações, órgãos públicos e especialmente nos escritórios de advogados.

Importante destacar que a Proteção de Dados, inclusive nos meios digitais, passou a ser considerada como um dos direitos fundamentais do cidadão, se incorporando à Constituição como uma cláusula pétrea, ou seja, não pode ser alterada.

As novas regras devem ser adotadas em todas as atividades do escritório que utilizem tratamento de dados, como nos contratos de honorários, contratos de trabalho, contratos de prestação de serviço, contratos com os parceiros de negócios, minutas, petições, pareceres, etc.

Juntamente com o Marco Civil da Internet e da Lei Geral da Proteção de Dados (LGPD), a nova emenda constitucional conclui a "arquitetura normativa" que todos os escritórios de advogados precisam estar em conformidade.

Caso não sejam observadas as normas, durante toda a vida útil dos dados pessoais, nas operações que envolvam tratamento de dados pessoais, poderão ser aplicadas sanções administrativas, previstas no artigo 52, aos escritórios de advogados que vão desde uma advertência, ao bloqueio de dados pessoais, a suspensão temporária ou a proibição da atividade de tratamento de dados pessoais até a aplicação de multa simples de até 2% do faturamento no seu último exercício, excluídos os tributos, limitada a R$ 50.000.000,00 por infração e ainda multa diária, respeitado o limite do da LGPD. As sanções podem ocorrer também na esfera judicial e já há mais de 1000 decisões judiciais com fundamento na proteção de dados e segurança da informação.

Esta obra foi composta em Calibri
em agosto de 2022.

Vivemos a era da revolução digital, na qual quem não se digitalizar a médio e longo prazo dificilmente permanecerá no mercado.

Já é impossível estabelecer modelos de negócios ou inovação tecnológica sem considerar o conceito de Privacy by Design.

Toda e qualquer empresa precisa incorporar salvaguardas de privacidade e proteção de dados pessoais em todos os projetos desenvolvidos.

Não há solução mágica, tampouco um caminho único para adequar uma organização à Lei Geral de proteção de Dados - LGPD. Cada modelo de negócio demanda um olhar específico. Um especialista poderá auxiliar a encontrar o melhor caminho.

Tenha em mente, porém, que a adequação à LGPD é fundamental para a sobrevivência do seu negócio e que somente trará resultados satisfatórios se for entendida como uma jornada multidisciplinar – com benefícios diretos na relação com empregados, clientes, fornecedores e terceiros – e não um projeto com data para iniciar e terminar.

Assim como um empresário precisa sempre cumprir a legislação trabalhista numa relação de trabalho, ou o CDC numa relação de consumo, todo e qualquer agente que tratar dados sempre terá de cumprir a LGPD para evitar passivos e que sejam aplicadas punições judiciais ou administrativas.

LIFE EDITORA

OAB MATO GROSSO DO SUL

ISBN 978-65-5887-136-1