EXCERTOS À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

SUMÁRIO

1 INTRODUÇÃO

O "General Data Protection Regulation" (GDPR), nº 2016/679, criado e aprovado pelo Parlamento Europeu e Conselho da União Europeia, é o regulamento do direito europeu que versa sobre a privacidade e proteção de dados pessoais, aplicável aos indivíduos da União Europeia e, inclusive, ao Espaço Econômico Europeu.

Inspirada na GDPR, o Brasil aprovou, em 10 de julho de 2018, a Lei Geral de Proteção de Dados (LGPD), nº 13.709/2018, sancionada em 14 de agosto de 2018. A LGPD entrará em vigor vinte e quatro meses após a data de sua publicação, ou seja, em meados de agosto de 2020, conforme determina o texto de lei.

Esta Lei regulamenta a forma pela qual as organizações, situadas no Brasil, passarão a utilizar os dados pessoais enquanto informação relacionada à pessoa natural, sendo ela identificada ou identificável.

A regulação brasileira estabelece normas rigorosas para a proteção dos dados pessoais, inclusive no que diz respeito ao tratamento dos dados coletados. Em suma, todas as empresas, sem exceção, que de alguma maneira fazem o tratamento de dados pessoais, deverão adotar uma série de medidas (políticas corporativas, recursos tecnológicos adequados, criptografia avançada em dispositivos de armazenamento de dados, treinamentos) para garantir o cumprimento da nova legislação, evitando assim quaisquer danos que possam ser gerados a partir do seu descumprimento.

2 PRINCIPAIS CONCEITOS

Titular

É toda pessoa física, a quem se referem os dados pessoais coletados.

Consentimento

A lei define consentimento a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, inclusive este sendo de aplicação obrigatória.

Dados pessoais

São caracterizados como sendo quaisquer informações que possam levar à identificação de uma pessoa natural, seja direta ou indiretamente (identificada ou identificável). Podemos citar como exemplo a referência a um nome, a um número de identificação (CPF, RG, CNH) ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social. Estes dados fazem referência, inclusive, aos dados coletados via internet (IP, dados de localização GPS, etc).

Dados pessoais sensíveis

Já, dados pessoais sensíveis são aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referentes à saúde, à vida ou orientação sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural. Vale mencionar que estes dados são aqueles que, se eventualmente forem expostos ou compartilhados, podem causar impacto para a vida pessoal e/ou profissional.

Os dados pessoais sensíveis podem ser objeto de tratamento quando o Titular ou seu representante legal autorizá-lo, mediante a formalização de consentimento para finalidades específicas. Caso não haja consentimento do Titular, o tratamento dos dados pessoais sensíveis somente poderá ocorrer quando for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, que os dados pessoais permaneçam anônimos; d) exercício regular de direitos; e) proteção da vida ou da incolumidade física do Titular ou de terceiros; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; e g) garantia da prevenção à fraude e à segurança do Titular.

A LGPD não permite o tratamento de dados pessoais sensíveis para atender ao interesse legítimo do Controlador ou de terceiros ou mesmo para proteção do crédito, tal como ocorre com os dados pessoais em geral, não qualificados como sensíveis. O tratamento de dados pessoais de crianças e adolescentes deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. A única hipótese em que a LGPD permite a coleta de dados pessoais sem o consentimento de pais ou responsável legal é no caso da coleta necessária para

realizar contato com os pais ou responsável legal. Vale ressaltar que as mesmas regras são aplicáveis às crianças e adolescentes, ou seja, o tratamento de dados deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Controlador

É aquela pessoa, Jurídica ou Física, que coleta dados pessoais e detém poderes para todas as decisões em relação à forma e finalidade do tratamento dos dados.

Operador/processador

Toda aquela pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Agentes de tratamento

São aqueles nomeados controlador e o operador.

Tratamento de dados

Considerada toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados.

Dado anonimizado/anonimização

Aquele dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento e a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, respectivamente.

Banco de dados

Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Encarregado (DPO)

Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Uso compartilhado de dados

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

3 FUNDAMENTOS DA LGPD

O artigo 2º determina como fundamento da LGPD: a) o respeito à privacidade; b) a autodeterminação informativa; c) a liberdade de expressão, de informação, de comunicação e de opinião; d) a inviolabilidade da intimidade, da honra e da imagem; e) o desenvolvimento econômico e tecnológico e a inovação; f) a livre iniciativa, a livre concorrência e a defesa do consumidor; e g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4 APLICAÇÃO DA LEI

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais, coletados no território brasileiro ou que tenha como objetivo oferecer bens ou serviços a pessoas localizadas no Brasil, independentemente destes dados pessoais terem sido coletados offline ou online, em meios físicos ou digitais.

Ainda, importa dizer que, aplica-se independentemente do meio e/ou forma de tratamento dos dados, ou seja, impõe regras ao tratamento de dados realizado dentro ou fora da internet, utilizando ou não meios digitais. Também, se aplica a operações de tratamento que ocorrem fora do país, quando: a) os dados pessoais forem coletados no Brasil; b) os dados sejam relacionados a indivíduos localizados no território brasileiro; c) tiver por objetivo a oferta de produtos e/ou serviços ao público brasileiro.

Há exceções à aplicação da Lei. Não se aplicada a LGPD ao tratamento de dados pessoais quando: a) realizado por pessoa natural para fins particulares; b) realizado para fins jornalísticos ou artísticos ou acadêmicos; c) realizado para fins de segurança pública,

defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (que será objeto de lei específica); ou d) provenientes de fora do território nacional e que não seja objeto de comunicação, uso compartilhado com agentes de tratamento brasileiros ou objeto de transferência de dados com outro país que não o de proveniência, desde que este país de proveniência proporcione grau de proteção adequado aos da lei brasileira.

5 PRINCÍPIOS APLICÁVEIS

Qualquer atividade de tratamento de dados pessoais observará, além da boa-fé, os seguintes princípios:

Finalidade

O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, observadas as finalidades originárias.

Adequação

O tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Necessidade

O tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Livre acesso

É garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Qualidade dos dados

É garantido aos titulares que seus dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Transparência

É garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Segurança

Devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenção

Devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Responsabilização e prestação de contas

Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas

6 DIREITOS DO TITULAR

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

O titular tem o direito de obter do controlador, em relação aos seus dados, a qualquer momento e mediante requisição: a) acesso aos dados; b) correção de quaisquer informações incorretas; c) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; d) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; e) informação das entidades públicas e privadas

com as quais o controlador realizou uso compartilhado de dados; f) revogação do consentimento.

É permitido, ainda, ao Titular peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

7 OBRIGAÇÕES DO CONTROLADOR

O Titular dos dados coletados pode exigir do Controlador, conforme previsão legal: a) provar que o consentimento foi obtido em conformidade com a LGPD; b) manter registro das operações de tratamento de dados pessoais que realize; c) mediante solicitação da autoridade nacional de proteção de dados, elaborar relatório de impacto à proteção de dados; d) informar o titular caso haja alguma alteração na finalidade para a coleta de dados; e) responder solidariamente, em conjunto com o operador, se causar a terceiros danos por violação da LGPD.

Além disso, está o Controlador obrigado a confirmar a existência ou providenciar o acesso a dados pessoais, mediante requisição do titular, em formato simplificado, imediatamente, ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até 15 (quinze) dias.

Manter registro das operações de tratamento de dados pessoais que realize, podendo a autoridade nacional determinar que seja elaborado relatório de impacto à proteção de dados (pessoais ou sensíveis) referente às suas operações. Caso venha a ocorrer esta solicitação, por parte da autoridade responsável, deve constar no relatório a descrição dos tipos de dados coletados, metodologia utilizada para a coleta de dados, metodologia utilizada para garantir a segurança das informações, análise do controlador com relação a essas medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

8 VAZAMENTO DE DADOS

Inicialmente insta dizer que o responsável pela coleta dos dados deve adotar medidas de segurança com a finalidade de garantir a proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou até mesmo ilícitas. Se mesmo assim ocorrer vazamento de dados (incidentes de segurança), indiferente do motivo ou meio, deve o responsável comunicar o mais breve possível a autoridade nacional de proteção de dados, bem como ao titular dos dados e órgãos reguladores setoriais.

Nesta comunicação devem constar, no mínimo, as seguintes informações: a) descrição da natureza dos dados pessoais afetados; b) os titulares envolvidos; c) as medidas técnicas e de segurança utilizadas para a proteção dos dados; d) os riscos relacionados ao incidente; e) os motivos da demora, no caso de a comunicação não ter sido imediata; f) as medidas adotadas para reverter ou mitigar os efeitos do prejuízo causado pelo incidente.

9 SEGURANÇA E PREVENÇÃO

As informações classificadas como pessoais requerem proteção adequada de forma a manter o sigilo e a privacidade de seu proprietário, requerendo para isto diversas medidas técnicas de proteção utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Ainda, para a devida prevenção é necessário a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

10 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei, ou seja, autoridade pública autônoma e independente para a supervisão da aplicação de lei, nomeada como Autoridade Nacional de Proteção de Dados – ANPD.

Órgão integrante da Presidência de República, criado a partir da sanção, em 27 de dezembro de 2018, da Medida Provisória nº 869/18 (que já sofreu alterações pela Medida Provisória 870/19), possuindo os poderes de fiscalização e aplicação de sanções no caso de descumprimento.

A Autoridade poderá estabelecer diretrizes para a promoção da proteção de dados pessoais no Brasil. Em resumo, esta deverá zelar pela proteção dos dados pessoais, elaborar a "Política Nacional de Proteção de Dados e da Privacidade", como definida pela lei, fiscalizar e aplicar sanções em caso de violação às leis pertinentes, atender petições de titulares de dados contra os responsáveis pelo seu tratamento, regulamentar as matérias sobre proteção de dados, entre outras atividades, ou seja, elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade, fiscalizar e aplicar sanções, promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança, e promover ações de

cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional.

A LGPD prevê também a criação do Conselho Nacional de Proteção de Dados, órgão consultivo, com composição multisetorial, que pode propor diretrizes e estratégias, realizar estudos e disseminar conhecimento sobre proteção de dados no Brasil.

11 DATA PROTECTION OFFICER (DPO)

O DPO foi traduzido pela LGPD como o "encarregado". É a pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a Autoridade Nacional. Ademais, deve ser o responsável dentro da instituição pela supervisão do cumprimento das regras previstas na lei e orientar os colaboradores e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. Será o responsável por disseminar a cultura de proteção de dados na empresa, além de criar normas e procedimentos adequados à lei. Será ele quem receberá notificações da ANPD e dos titulares das informações e as colocará em prática.

12 RELATÓRIO DE IMPACTO À PRIVACIDADE - DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Conceituado como o "relatório de impacto à proteção de dados pessoais", refere-se à documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos direitos dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos. Poderá ser obrigatório em situações já caracterizadas como de risco ou, a pedido da Autoridade reguladora, quando o tratamento de dados for baseado no legítimo interesse. A metodologia do DPIA é amplamente adotada pela GDPR e permite, além do mapeamento dos riscos, uma efetiva fotografia do status da conformidade regulatória.

13 RELAÇÕES DE TRABALHO E EMPREGO

Tendo em vista que o empregador é detentor de informações pessoais de seus empregados, a LGPD deve ser observada em sua totalidade, sob pena de responsabilidade civil, além de ressarcimento de eventuais danos causados.

Embora a LGPD autorize as empresas a usar os dados pessoais dos seus empregados e prestadores de serviços para a legítima execução dos contratos, em

benefício do próprio trabalhador, não se pode desconsiderar cautela e observância das regras da Lei em comento em todas as suas fases, nos atos praticados antes da contratação, durante a vigência do contrato, nas terceirizações e após a rescisão dos contratos.

Em situações práticas, deve o empregador requerer o consentimento expresso do candidato e informá-lo de maneira clara que seus dados serão utilizados para recrutamento, avaliação e seleção. Todavia, no caso de não ser contratado, a empresa deverá eliminar os dados pessoais obtidos, ressalvadas as hipóteses de obrigação legal de conservar tais documentos.

É extremamente importante que o empregado/colaborador/prestador esteja ciente do uso dos seus dados pessoais, autorizando a utilização para a realização de todas as ações relacionadas a seu contrato de trabalho/prestação de serviços. Este consentimento para tratamento dos dados pessoais do empregado/prestador de serviços pode estar previsto no contrato, desde que em cláusula individualizada e devidamente destacada.

Vale mencionar que autorizações genéricas serão consideradas nulas, bem como alterações relacionadas ao tratamento das informações que não forem comunicadas ao Titular. A LPD dispensa o consentimento do empregado no tratamento de dados pessoais indispensáveis ao cumprimento de obrigações legais ou regulatórias pelo empregador, por exemplo, o envio de dados ao Ministério do Trabalho e Emprego (atualmente Ministério da Economia), INSS e CEF, por meio dos documentos denominados CAGED, RAIS E SEFIP.

Empregadores que só tratam dados pessoais indispensáveis para o exercício de atribuições legais e regulatórias precisam enviar um comunicado aos empregados, informando especificamente: a) quais dados são tratados; b) quais obrigações serão cumpridas com esses dados; e c) com quais entidades públicas os dados serão compartilhados.

Por fim, encerrada a relação de trabalho, os dados pessoais do trabalhador/prestador devem ser eliminados, salvo nas hipóteses de obrigação legal de conservar tais documentos. Nos casos de terceirização de serviços, é preciso obter consentimento dos empregados/prestadores, por escrito, para que a empresa faça o tratamento dos seus dados, sobretudo quando for transmiti-los a terceiros (tomadores de serviço), em decorrência da atividade realizada, ou mesmo por exigências legais e contratuais, especificando de maneira clara quais dados serão repassados e para qual finalidade.

14 SANÇÕES

A parte mais crítica e importante da LGPD diz respeito às sanções que podem ser impostas ao Controlador. O descumprimento das normas estabelecidas, pelos agentes de tratamento de dados, em razão das infrações cometidas, vão desde advertência até a imposição de sanções de natureza pecuniária, que podem gerar multas simples, de até 2% (dois por cento) do faturamento TOTAL 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 e/ou multa diária, observado o limite total acima mencionado, além da responsabilidade de indenizar o titular dos dados.

Vale destacar que as sanções podem ser aplicadas cumulativamente, por dia e infração, mas sempre com base na gravidade e extensão da violação.

Para estabelecer as sanções, observada a ampla defesa do infrator, serão aplicados considerando as particularidades de cada caso, os seguintes parâmetros e critérios: a) gravidade e a natureza das infrações e dos direitos pessoais afetados; b) boa-fé do infrator; c) vantagem auferida ou pretendida pelo infrator; d) condição econômica do infrator; d) reincidência; e) grau do dano; f) cooperação do infrator; g) adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano; h) adoção de política de boas práticas e governança; i) pronta adoção de medidas corretivas; j) proporcionalidade entre a gravidade da falta e a intensidade da sanção.

15 CONCLUSÃO

A LGPD terá um impacto substancial na sociedade, tendo em vista que, atualmente, toda e qualquer prática se vale do uso de dados pessoais. Dito isso, é importantíssimo que as empresas (de todos os setores) se adaptem a essa nova cultura sobre o uso adequado de dados. Claramente, a lei geral de proteção de dados representa um passo necessário e importante. À primeira vista para demonstrar que o Brasil está em posição equânime com diversos países que já possuem tratamento definido sobre o tema, além de demonstrar que a Legislação pátria exige bom senso e transparência de quem lida com dados pessoais, procurando penalizar excessos e abusos através da definição da responsabilidade e do dever de indenizar. Sem dúvida, cria confiança jurídica aos cidadãos brasileiros, mas também àqueles que pretendem investir de alguma forma no país.

Por fim, importa destacar que a MP 869/2018, que altera a LGPD, ainda está sendo analisada no Congresso. O relatório da comissão mista que está tratando desse assunto foi aprovado em 07/05/2019, ou seja, em breve será levado ao plenário para votação onde há a possibilidade de novas alterações envolvendo a LGPD e a criação da Autoridade Nacional de Dados.

REFERÊNCIAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 03 de abril de 2019.

COMISSÃO Especial da Lei Geral de Proteção de Dados (LGPD). **FEDERASUL**. [2019?]. Disponível em <https://www.federasul.com.br/wp-content/uploads/2019/01/Comiss%C3%A3o-Especial-da-Lei-Geral-de-Prote%C3%A7%C3%A3o-de-Dados-LGPD-1.pdf>. Acesso em 03 de abril de 2019.

COTS, Marcio. LGPD: entenda a Lei Geral de Proteção de Dados no e-commerce. **E-commercebrasil**. 22 de agosto de 2018. Disponível em <https://www.ecommercebrasil.com.br/artigos/lei-geral-de-protecao-de-dados-e-commerce/>. Acesso em 03 de abril de 2019.

GUIA para a Lei Geral de Proteção de Dados. **Mattos Filho, Veiga Filho, Marrey Jr. E Quiroga Advogados**. Agosto de 2018. Disponível me <https://www.legiscompliance.com.br/images/pdf/cartilha_lgpd_mattosfilho.pdf>. Acesso em 01 de abril de 2019.

LEI 13.709/18 - Lei de Proteção de Dados Pessoais. **Machado e Mayer Advogados**. Agosto de 2018. Disponível em <https://www.machadomeyer.com.br/images/publicacoes/PDFs/Lei_Protecao_de_Dados_ebook_18.pdf>. Acesso em 03 de abril de 2019.

LEI Geral de Proteção de Dados brasileira e seus impactos para empresas. **AB2L (Associação Brasileira de Lawtechs e Legalthecs).** 13 de janeiro de 2019. Disponível em <https://www.ab2l.org.br/lei-geral-de-protecao-de-dados-brasileira-e-seus-impactos-para-empresas/>. Acesso em 03 de abril de 2019.

LEI Geral de Proteção de Dados do Brasil – Análise. **Batista Luz Advogados**. 18 de julho de 2018. Disponível em <https://baptistaluz.com.br/institucional/lei-geral-de-protecao-de-dados-do-brasil-analise/>. Acesso em 03 de abril de 2019.

LEI Geral de Proteção de Dados: Um Resumo da LGPD. **LegalCloud**. 29 de agosto de 2018. Disponível em <https://legalcloud.com.br/lei-geral-de-protecao-de-dados-resumo-lgpd/>. Acesso em 02 de abril de 2019.

MANUAL Normativo: Lei Geral de Proteção de Dados e GDPR. **Batista Luz Advogados**. 30 de janeiro de 2019. Disponível em <https://baptistaluz.com.br/institucional/manual-normativo-lei-geral-de-protecao-de-dados-e-gdpr/>. Acesso em 03 de abril de 2019.