LEI GERAL DE PROTEÇÃO DE DADOS

Cartilha LGPD

Junho de 2021

Há mais de 60 anos, o Instituto Brasileiro de Petróleo e Gás atua como representante da indústria de Óleo e Gás. O Instituto preza pelo consenso entre os diversos atores da indústria a partir de ações e práticas isentas, apartidárias e transparentes, guiadas sempre pela ética e transparência.

Ao longo dessas seis décadas, entre as prioridades do IBP está o respeito aos consumidores, parceiros, fornecedores e demais públicos que seguem lado a lado nesta jornada ajudando a construir uma história de sucesso.

Parte do compromisso primordial do IBP envolve o respeito às informações pessoais e confidenciais compartilhadas e/ou acessadas, sejam elas de colaboradores ou de parceiros.

A partir da Lei Geral de Proteção de Dados (13.709/2018), a proteção e a preservação de tais informações tornaram-se um compromisso de ordem não apenas ética, mas jurídica e institucional, essencial na preservação e na promoção do respeito à privacidade e a dados pessoais.

Como parte do trabalho de gestão de conhecimento e acessibilidade às informações, o IBP apresenta a Cartilha LGPD, na qual os interessados poderão aprofundar seus conhecimentos e esclarecer suas dúvidas sobre o tema.

O objetivo deste material é gerar conhecimento e auxiliar empresas e pessoas físicas na preservação e na proteção de dados.

Boa leitura!

Trabalho organizado pelo Comitê de Gestão de Pessoas do IBP em parceria com os escritórios jurídicos:

www.cmalaw.com
Participação: Mauricio Tanabe e Paula Mena Barreto
E-mail(s): mauricio.tanabe@cmalaw.com e paula.menabarreto@cmalaw.com
Telefone: +55 21 3077-3521

www.coelhodalle.com.br
Participação: Ana Carolina Lessa, Diogo Araújo, Felipe Medeiros, Jamille Santos e Mariana Gusmão
E-mail(s): eduardocoelho@coelhodalle.com.br e ricardodalle@coelhodalle.com.br
Telefone(s): + 55 81 3221-0699 e +55 11 3728-9223

www.mattosfilho.com.br
Participação: Thiago Luís Sombra e Rafael de Filippis
E-mail(s): rafael.filippis@mattosfilho.com.br e thiago.sombra@mattosfilho.com.br
Telefone: +55 21 3231 8200

Sumário

ENTENDENDO A LGPD 5

A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS 11

CENÁRIO EXTERIOR 12

COMO APLICAR A LGPD 14

FORNECEDORES E PRESTADORES DE SERVIÇOS 16

COLETA DE DADOS 17

AVALIAÇÃO, PROCESSOS, CONTRATOS E FASES 19

TRATAMENTO DE DADOS E INFORMAÇÕES 22

CONSCIENTIZAÇÃO E CONTROLE DA LGPD 24

OS TRÊS INTERLOCUTORES 27

LEGITIMAÇÃO E BASES LEGAIS 31

EM CASO DE IRREGULARIDADES OU DESLIGAMENTO 33

ENTENDENDO A LGPD

Por que foi criada a LGPD (Lei nº 13.709/2018)?

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018, "LGPD") foi criada com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, e o livre desenvolvimento da personalidade da pessoa natural, estabelecendo mecanismos para proteger os titulares dos dados contra usos inadequados. Assim, a LGPD foi criada com o intuito de dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como à proteção dos direitos individuais, no que tange à privacidade.

A aprovação da LGPD e a criação da Autoridade Nacional de Proteção de Dados (ANPD) representam também importantes passos para colocar o Brasil no mesmo patamar de muitos outros países que já aprovaram leis e estruturas institucionais dessa natureza. A constituição de um ambiente jurídico voltado à proteção de dados pessoais corresponde ainda ao alinhamento com diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que há décadas vem desempenhando relevante papel na promoção do respeito à privacidade como valor fundamental e como pressuposto para o livre fluxo de dados.

Por fim, do ponto de vista dos agentes de tratamento de dados, sejam empresas ou o próprio poder público, a LGPD traz a oportunidade de aperfeiçoamento das políticas de governança de dados, com adoção de regras de boas práticas e incorporação de medidas técnicas e administrativas que mitiguem os riscos e aumentem a confiança dos titulares dos dados na organização.

Quando entrou em vigor?

A Lei entrou em vigor no dia 20 de setembro de 2020, após diversas discussões e postergações. Contudo, é importante notar que as penalidades previstas pela lei apenas entrarão em vigor no dia 1º de agosto de 2021.

Quais são os direitos protegidos pela LGPD?

Fortemente inspirada nas disposições do *General Data Protection Regulation* (GDPR), a LGPD garantiu a criação de diversos direitos aos titulares de dados e estabeleceu novos parâmetros para o tratamento de dados pessoais. Conforme estabelece o Artigo 1º da LGPD, seu objetivo é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ainda, a LGPD estabelece direitos específicos para o titular de dados pessoais, quais sejam: **(i)** acesso facilitado às informações sobre o tratamento de seus dados; **(ii)** confirmação da existência de tratamento; **(iii)** correção de dados incompletos, inexatos ou desatualizados; **(iv)** anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; **(v)** portabilidade dos dados; **(vi)** eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Art. 16 da LGPD; **(vii)** informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; **(viii)** informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e **(ix)** revogação do consentimento.

A LGPD tem a finalidade de proteger os direitos fundamentais relacionados à esfera informacional do cidadão (seus dados pessoais, como, nome, endereço, CPF, RG, CTPS, Título de Eleitor, e-mail, IP, entre outros). Assim, a Lei introduz uma série de novos direitos que asseguram maior transparência quanto ao tratamento dos dados e conferem protagonismo ao titular quanto ao seu uso.

O que e quem será impactado pela LGPD?

A LGPD garante proteção a todos os dados cujos titulares são pessoas naturais, estejam eles em formato físico ou digital. Assim, a LGPD não alcança os dados titularizados por pessoas jurídicas – os quais não são considerados dados pessoais para os efeitos da Lei. Titulares de dados agora possuem a garantia do melhor tratamento de seus dados pessoais e agentes de tratamento de dados pessoais deverão atentar aos novos requisitos legais para esses processamentos.

De acordo com seu Artigo 4º, salvo algumas exceções, a LGPD 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, desde que: **(i)** o tratamento de dados pessoais ocorra no território nacional; **(ii)** a atividade de tratamento de dados pessoais destine-se a oferecer ou fornecer bens ou serviços a ou tratar dados de indivíduos localizados no Brasil; ou **(iii)** os dados pessoais objeto do tratamento tenham sido coletados no Brasil.

Em quais setores a LGPD se aplica e não se aplica?

A LGPD não distingue sua aplicação a determinados setores e, dessa forma, vai se aplicar sempre que: **(i)** a operação de tratamento seja realizada no Brasil; **(ii)** a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil; ou **(iii)** os dados pessoais objeto do tratamento tenham sido coletados no Brasil.

Conforme seu Artigo 4º, a LGPD prevê algumas opções em que não se aplica ao tratamento de dados pessoais realizado nos seguintes casos: **(i)** por pessoa natural para fins exclusivamente particulares e não econômicos; **(ii)** para fins exclusivamente jornalísticos ou artísticos; **(iii)** para fins exclusivamente acadêmicos, salvo algumas previsões da lei; e **(iv)** para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais. Além disso, não se aplica a LGPD aos dados pessoais 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

Como aplicar os requisitos básicos da LGPD ao nosso negócio? Exemplo: qual o roteiro básico por onde começar? Quais são as fases de implementação? É possível fornecer um guiazão com, por exemplo, 10 etapas para a LGPD ser efetiva na sua implementação e manutenção?

Os requisitos da LGPD devem ser observados por todas as áreas que tratem dados pessoais de pessoas físicas em suas atividades. Dessa forma, a sua aplicação deverá ser avaliada conforme o cenário factual de cada empresa. Em geral, será necessário inicialmente mapear todas as atividades realizadas pelas áreas em um inventário de tratamento de dados pessoais, de modo a desenvolver plano de ação específico e direcionado aos pontos de atenção da empresa.

A LGPD estabelece uma série de medidas que devem ser adotadas pelos agentes de tratamento. Tais medidas devem se concretizar com ações que envolvem o mapeamento dos dados; a revisão dos contratos e documentos jurídicos; a elaboração de políticas de privacidade e termo de uso; a implementação de *compliance* e governança; e, principalmente, a realização de treinamento das equipes, conscientizando-as sobre a proteção dos dados pessoais.

A Lei determina ainda que os controladores de dados indiquem um encarregado (*Data Protection Officer - DPO*) para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Em determinadas circunstâncias, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados, a ANPD poderá estabelecer hipóteses de dispensa da necessidade de sua indicação.

Enfim, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Por fim, é relevante pontuar que a ANPD ainda regulará sobre diversos temas da LGPD, o que pode ter impacto na adequação das empresas à lei, de modo que elas deverão se manter constantemente atentas a seu pronunciamento.

Não há um manual único de implementação da LGPD. As empresas precisam se adequar de acordo com as suas necessidades específicas.

Qual o período correto de armazenamento de dados de Colaboradores e pessoas externas? O que armazenar?

A LGPD não determina os períodos de armazenamento de diferentes tipos de dados e/ou documentos. O controlador poderá armazenar os dados pessoais enquanto não for verificada uma das hipóteses de eliminação de dados pessoais previstas na LGPD (Art. 15, LGPD). A Lei estipula que os dados pessoais deverão ser eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as finalidades de: **(i)** cumprimento de obrigação legal ou regulatória pelo controlador; **(ii)** estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; **(iii)** transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou **(iv)** para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Desta forma, os dados poderão ser mantidos desde que para finalidades específicas e determinadas. Após atingir o cumprimento desta finalidade, os dados deverão ser armazenados conforme o prazo necessário para cumprimento de obrigação legal ou regulatória - tal como para fins de obrigações previdências pelo empregador, por exemplo.

Nos termos da Lei, a Autoridade Nacional (ANPD) poderá dispor sobre padrões do tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

É possível a postergação da aplicação de penalidades administrativas após agosto de 2021?

Existe em tramitação, na Câmara dos Deputados, Projeto de Lei (500/2021, apensado ao PL nº 5.762/2019), que visa a postergar, para 1º de janeiro de 2022, a entrada em vigor das multas às empresas que descumprirem a Lei Geral de Proteção de Dados. Mas ainda não houve deliberação do Órgão Legislativo sobre o assunto.

No entanto, é relevante notar a movimentação da ANPD (Autoridade Nacional de Proteção de Dados) no âmbito de regulamentar a fiscalização e aplicação de sanções. A ANPD publicou, em 28 de maio de 2021, minuta de resolução que foi submetida à consulta pública e pretende regulamentar a aplicação do Artigo 52 e seguintes da LGPD. O documento indica os mecanismos de fiscalização que a ANPD pretende adotar, por meio de ações de monitoramento, orientação, prevenção e aplicação de sanções. O texto apresentado detalha ainda todas as fases do processo administrativo sancionador e suas fases. Nesse sentido, percebe-se que o cenário para uma nova postergação da aplicabilidade das sanções é diverso: agora, ao contrário do que havia em 2020, quando houve a primeira postergação, temos órgão regulador estruturado para a aplicação das sanções.

O que é dado pessoal sensível e qual a diferença para um dado confidencial? Como tratar cada um deles?

Dado pessoal sensível, conforme definido pela LGPD, é um dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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.

Os dados confidenciais são aquelas informações acessíveis a apenas um grupo de pessoas autorizadas. Pode abarcar um dado sensível.

O tratamento de dados pessoais sensíveis deve ser precedido de cautelas maiores, com especial atenção aos princípios e direitos dos titulares, uma vez que eventual incidente de segurança com esses tipos de dados pode trazer consequências mais gravosas aos direitos e liberdades dos titulares.

É importante destacar que a principal diferença entre o tratamento de dados pessoais e dados pessoais sensíveis é que, nessa última, como regra, a base legal aplicada é o consentimento, de forma específica e destacada, para finalidades específicas. Dessa forma, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger

os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito nos termos do Artigo 46 da LGPD.

A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Quais indicações a ANPD (Autoridade Nacional de Proteção de Dados) irá seguir do Manual da Legislação Europeia sobre Proteção de Dados?

Apesar de ter sido fortemente influenciada pelo GDPR (*General Data Protection Regulation*), a LGPD possui diferenças suficientes para que não seja possível implementar as mesmas orientações de forma literal.

Atualmente, o GDPR é um dos regulamentos de proteção de dados com orientações mais claras e deve servir de forte inspiração para as regras a serem elaboradas pela ANPD. Entretanto, as diferenças entre as leis e realidades dos países podem resultar em implementações diferentes.

A ANPD ainda está realizando os estudos de aplicação da LGPD, de modo que ainda não está bem definido o que será seguido ou não do Regulamento Europeu. A tendência é que existam alinhamentos nos princípios compartilhados entre as duas legislações, por exemplo: interpretações da aplicação do princípio da transparência e orientações gerais de melhores práticas.

A ANPD recebe consultas feitas de forma proativa?

Já é possível apresentar documentos perante a ANPD de forma eletrônica. No entanto, ainda não há regulamentação ou posicionamento da ANPD acerca de consultas, visto que a Autarquia ainda está em fase de estruturação. Diante desse cenário, ainda não é possível determinar os riscos de uma consulta formal.

A realização de uma consulta formal à ANPD possui benefícios e riscos. Como benefícios, o controlador tem a possibilidade de apresentar de modo claro e explicativo o seu novo produto e/ou seu ponto de vista, demonstrando estar de boa-fé e receptivo ao diálogo com a autoridade – o que é positivo para evitar eventuais sanções posteriores. Por outro lado, as consultas proativas podem ser arriscadas a partir do momento em que não é possível prever o entendimento que será formulado pela autoridade, ou seja, a consulta servirá para chamar a atenção da autoridade para um tema que poderia passar despercebido por ela.

CENÁRIO EXTERIOR

Em caso de empresas sediadas no exterior, mas que oferecem bens e/ou serviços para pessoas localizadas no Brasil, a LGPD também se aplica?

Sim. Conforme estipulado no Artigo 3º da LGPD, a lei se aplicará sempre que: (i) a operação de tratamento seja realizada no Brasil; (ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil; ou (iii) os dados pessoais objeto do tratamento tenham sido coletados no Brasil. Desta forma, mesmo que uma empresa seja sediada no exterior ou que tenha acesso ou receba dados coletados no Brasil, ela estará sujeita às obrigações da lei brasileira de proteção de dados.

Como as empresas estão tratando as informações que remetem para as matrizes no exterior (exemplo: informações de funcionários)? Como o mercado tem utilizado os mecanismos de transferência previstos na LGPD nas suas transferências internacionais nesse momento em que ainda não há normatização da ANPD?

O compartilhamento de dados pessoais por entidades localizadas no Brasil com entidades sediadas no exterior configura uma transferência internacional de dados nos termos da LGPD e, por consequência, exige que os controladores de dados atendam a requisitos específicos. Entre outras hipóteses, a LGPD estabelece que transferências internacionais de dados são permitidas: (a) para países ou organizações internacionais que oferecem nível adequado de proteção a dados pessoais, conforme a ser determinado pela ANPD; (b) quando o controlador oferecer e comprovar garantias de cumprimento da LGPD, por meio de cláusulas contratuais específicas para determinada transferência, cláusulas contratuais padrão, normas corporativas globais ou certificados e códigos de conduta, todos devidamente aprovados pela ANPD; (c) quando autorizada a transferência pela ANPD; (d) quando o titular fornecer seu consentimento específico e em destaque para a transferência, tendo sido fornecida informação prévia e distinta de outras finalidades sobre o caráter internacional da operação; (e) quando necessário para cumprimento de obrigação legal ou regulatória pelo controlador; (f) para execução de contrato ou procedimentos relacionados ao contrato do qual seja parte o titular, desde que requerido pelo próprio titular; ou (g) para exercício regular de direitos em processo judicial, administrativo ou arbitral.

Parte dos mecanismos internacionais de transferência de dados elencados acima requer regulamentação adicional da ANPD. Apesar da ausência de diretrizes, para fins de demonstração de boas práticas e zelo com a legislação, o controlador de dados, ao compartilhar dados pessoais com entidades localizadas no exterior, pode se valer dos mecanismos descritos acima. Alinhada com a experiência europeia, quando a transferência for realizada com entidade integrante do grupo econômico/conglomerado, deve-se estabelecer normas corporativas vinculantes (*Binding Corporate Rules* – BCRs) para regular a transferência internacional de dados, que são códigos internos que se aplicam a todo conglomerado financeiro ou grupo econômico de caráter internacional. Tais regras devem – como o próprio nome sugere – ser juridicamente vinculantes e aplicáveis a todas as entidades pertencentes ao conglomerado financeiro ou ao grupo econômico. Tão logo seja possível, as referidas BCRs devem ser submetidas à aprovação da ANPD.

COMO APLICAR A LGPD

Quais seriam as recomendações em caso de tratamento de dados realizados com amparo em outras bases legais e não no consentimento? Quais seriam as recomendações para atender ao princípio da transparência?

O uso de qualquer uma das bases legais deverá ser realizada com observância dos requisitos da LGPD, tal como os princípios da transparência, adequação e necessidade. Nesse sentido, as bases legais adotadas – tanto o consentimento do titular quanto as demais estipuladas no Artigo 7º ou 11º — deverão estar apontadas no inventário de tratamento de dados pessoais da empresa para cada finalidade de tratamento. Igualmente, é recomendável garantir a transparência desses processamos e a forma da utilização dos dados pessoais nas políticas e avisos de privacidades adequadas aos titulares.

O princípio da transparência corresponde a uma garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. Nesse sentido, para fins de atendimento a tal princípio, o controlador deverá implementar políticas de privacidade para apresentar informações claras e completas aos titulares de dados sobre: (a) a finalidade do tratamento de dados; (b) a forma e duração do tratamento; (c) a identificação e contato do controlador; (d) as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e a respectiva finalidade de tal uso compartilhado; e (e) direitos que o titular poderá exercer, entre outras informações relevantes. Ademais, tais políticas deverão ser de fácil acesso aos titulares de dados pessoais.

Há documento único que cubra parte ou totalmente as exigências da LGPD de forma que os dados possam ser usados pelas empresas de modo a agilizar e evitar trabalhos administrativos desnecessários?

Não. Ressalta-se que a proteção de dados dentro das empresas deve ser mudança de atitude institucional com relação aos dados pessoais tratados. Os documentos servirão apenas para formalizar isso. Ainda não se sabe com detalhes como serão exigidas as regras de proteção de dados e os documentos que serão eventualmente solicitados. Também há variação muito grande entre os níveis de proteção de dados e as medidas que as empresas devem tomar para se adequar, o que exige avaliação individualizada da realidade de cada uma.

O Brasil seria considerado uma jurisdição que observa as garantias mínimas exigidas pela GDPR (*General Data Protection Regulation*) e, portanto, poderia receber dados pessoais de operações de tratamento de dados realizados na Europa sem a necessidade de adoção de cláusulas específicas nos contratos? Há alguma discussão específica na ANPD sobre o assunto?

Não. Até o presente momento, o Brasil não é considerado uma jurisdição que observa as garantias mínimas exigidas pela GDPR. Desse modo, para que as empresas situadas no Brasil possam receber dados pessoais decorrentes de operações de tratamento realizadas na Europa, é necessário que elas adotem as cláusulas contratuais específicas para a transferência internacional de dados. De acordo com o Artigo 35 da LGPD, a definição do conteúdo de cláusulas contratuais específicas para determinada transferência será realizada pela ANPD. Além disso, na análise de cláusulas contratuais, a ANPD poderá solicitar informações suplementares ou diligências de verificação quanto às operações de tratamento. Entretanto, a ANPD ainda não se manifestou sobre esse assunto. De acordo com a Portaria nº 11, de 27 de janeiro de 2021 (a qual tornou pública a agenda regulatória da ANPD para o biênio 2021—2022), a ANPD irá regular o tema de transferência internacional de dados pessoais, no que tange aos Artigos 33, 34 e 35 da LGPD, por meio de resolução no primeiro semestre de 2022.

Qual o nível de publicidade e atualização periódica de boas práticas e de governança de dados exigidos pelo Art. 50, §3º, da LGPD? Todas as políticas internas da empresa sobre o assunto precisam ser publicadas ou apenas uma política de privacidade geral seria suficiente?

O Art. 50, §3º, da LGPD trata da publicação das regras de boas práticas e governança gerais da empresa. A princípio, a elaboração de uma política de boas práticas (ou utilização de uma já elaborada) é opcional, mas recomendável.

As regras de boas práticas poderão ser elaboradas por associações, ou outros grupos organizados, e implementadas nas empresas sem a necessidade de regras específicas para cada empresa. No caso de implementação formal de uma política de boas práticas, é recomendável que ela esteja disponível para consulta interna e publicada para consulta externa, mas não há regra clara sobre quais devem ser publicadas ou não.

Recomendamos que as políticas que disponibilizam informações do interesse de titulares, como quais dados serão tratados e com quem serão compartilhados, sejam publicadas. Procedimentos internos podem ser mantidos somente entre os Colaboradores interessados.

FORNECEDORES E PRESTADORES DE SERVIÇOS

Quais exigências devem ser apresentadas para os fornecedores e/ou prestadores de serviços externos em relação ao cumprimento da LGPD?

O nível de exigência vai depender do tipo de serviço ou bem fornecido e se os dados pessoais dos quais a empresa é controladora ou operadora vão ser compartilhados ou não com os fornecedores/prestadores.

Caso algum dado pessoal seja compartilhado, é preciso confirmar que o fornecedor/prestador está adequado à LGPD e possui a capacidade técnica de proteger os dados compartilhados. Recomenda-se a previsão contratual de auditoria de conformidade com a LGPD, inclusive com a possibilidade de solicitação de relatório de impacto.

A depender do risco do tratamento dos dados compartilhados, pode ser recomendável auditoria periódica no decorrer da relação contratual.

Em determinados períodos, devemos auditar nossos fornecedores e/ou prestadores de serviços para o cumprimento da LGPD? Quais documentos solicitamos para garantir o cumprimento da lei?

A depender do tipo e quantidade de dados pessoais compartilhados com os prestadores/fornecedores, é recomendável prever auditoria periódica de conformidade. Os períodos podem variar a depender do risco relativo aos dados compartilhados.

A LGPD não estabelece documento único que possa ser solicitado para confirmar a adequação de um prestador. A depender do tipo de serviço prestado, as sugestões de documentos a serem solicitados podem variar.

Ter uma política de privacidade e um mapeamento de dados já são bons sinais. Com relação aos dados pessoais que precisem de consentimento, é recomendável solicitar os documentos que confirmem que o consentimento foi dado.

A adequação com certificações também são documentos que podem ser apresentados. Certificação da família ISO 27000, para normas de gestão de segurança da informação, são demonstrativos de bom nível de adequação.

COLETA DE DADOS

Caso não tenhamos a ciência do empregado, podemos coletar e manter a informação em nossos arquivos? (considerando que as informações são necessárias para as entregas das obrigações trabalhistas.)

Sim. O consentimento é somente uma das bases legais previstas na LGPD que possibilitam o tratamento de dados pessoais e dados pessoais sensíveis. Há grande discussão sobre a validade da manifestação de vontade do empregado em relação à coleta do consentimento para o tratamento dos seus dados pessoais, haja vista que o colaborador se encontra em uma situação de subordinação. Tal situação pode inviabilizar a obtenção de um consentimento verdadeiramente livre, já que o colaborador pode se sentir implicitamente constrangido a aceitar qualquer condição que o empregador lhe apresente. Ainda que, na prática, o empregador dê a liberdade de o colaborador consentir ou não, sem qualquer constrangimento ou consequência negativa no caso de o colaborador não consentir, e o colaborador entenda tal situação, é difícil produzir essa prova em um eventual questionamento realizado por autoridades ou no âmbito do Poder Judiciário.

Assim, recomenda-se considerar outras bases legais menos onerosas para o empregador, como o cumprimento de obrigação legal ou regulatória prevista no Artigo 7º, II, da LGPD. Contudo, ressalta-se que, caso a empresa realize o tratamento de dados pessoais de crianças e adolescentes (como no caso dos jovens aprendizes), a LGPD estabelece que a empresa deverá obter o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Quando a finalidade da coleta de dados muda, o que a empresa deve fazer?

A LGPD estabelece que o tratamento de dados deverá observar o princípio da finalidade, isto é, deverá ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, nos termos do Artigo 6º, I, da LGPD. Na hipótese em que o consentimento é requerido ao titular dos dados, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Portanto, via de regra, se a empresa verificar que a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada, ela deverá encerrar o tratamento dos dados pessoais. Contudo, é autorizada a conservação dos dados pessoais para o cumprimento de obrigação legal ou regulatória pela empresa, uso exclusivo do controlador sendo vedado o seu acesso a terceiro e demais hipóteses elencadas no Artigo 16 da LGPD.

AVALIAÇÃO, PROCESSOS, CONTRATOS E FASES

Que tipo de avaliação/diagnóstico de LGPD vocês sugerem para cada empresa?

O diagnóstico de adequação deverá ser contínuo e tem o objetivo de apontar para a empresa o que deve ser aprimorado para sua adequação à LGPD. Recomendamos que o Encarregado: (i) acompanhe todos os processos que envolvam proteção de dados e privacidade dentro da empresa; (ii) atualize os registros de mapeamento dos dados quando necessário; (iii) certifique-se de que identificou e documentou o impacto potencial sobre a privacidade dos titulares por meio do Relatório de Impacto à Proteção de Dados, quando aplicável; e (iv) reporte os resultados do programa de adequação implementado. Ademais, é necessário que a empresa acompanhe e avalie as solicitações feitas pelos titulares dos dados a fim de atestar a maturidade da sua adequação perante essas solicitações (tais como pedido de acesso aos dados, portabilidade, exclusão, revogação do consentimento, entre outros previstos no Artigo 18 da LGPD). Somado a isso, recomendamos também que a avaliação inclua a gestão de incidentes, com a adoção de indicadores de monitoramento do número de incidentes de segurança e/ou vazamento de dados pessoais com a devida documentação dos eventos.

Para empresas B2B, a adequação e o diagnóstico da LGPD podem ser ainda mais desafiadores. Para essas empresas, recomendamos especial atenção em relação à avaliação e atualização das políticas de privacidade, atualização do consentimento fornecido pelos contatos de prospects da base de dados, revisão periódica do banco de dados, nomeação do Encarregado de Proteção de Dados e realização de treinamentos periódicos sobre proteção de dados e privacidade.

Com que periodicidade e como vocês sugerem avaliar o grau de maturidade da empresa em relação à LGPD?

Recomendamos que a avaliação do grau de maturidade da empresa em relação à LGPD ocorra periodicamente e nos casos específicos em que: (i) a ANPD publique e disponibilize resoluções e orientações específicas sobre os dispositivos da lei; (ii) ocorrer a alteração de algum processo dentro da empresa que coleta ou passe a coletar quantidade significativa de dados pessoais e/ou dados pessoais sensíveis; (iii) ocorrer algum incidente de segurança

envolvendo dados pessoais de colaboradores, clientes ou terceiros; (iv) seja implementado novo produto ou serviço que possa comprometer os direitos dos titulares, bem como os direitos e garantias fundamentais previstos nos Artigos 17 e 18 da LGPD; (v) ocorrer transferência internacional dos dados pessoais para outros países ou organismos internacionais; entre outros. Entendemos que a avaliação do grau de maturidade da empresa poderá ser realizada internamente por ela, mediante autoavaliação dos processos e procedimentos internos, como também por auditoria externa.

Quais seriam os processos mais críticos para a LGPD?

Em geral, são os processos que envolvem dados sensíveis, dados de menores e processos que possam gerar discriminação ou riscos ao titular.

Os processos mais críticos para a LGPD dentro de uma empresa são aqueles processos que envolvem o tratamento significativo de dados pessoais e/ou dados pessoais sensíveis em departamentos como RH, Marketing e Jurídico. A título de exemplo, podem ser citados os processos: (i) processos seletivos para candidatos a vagas de emprego; (ii) admissão de novos colaboradores; (iii) adesão ao plano de previdência; (iv) participação em grupos de diversidade e afinidade; (v) envio de e-mail marketing aos usuários do site ou clientes da empresa; e (vi) coleta de dados pessoais de representantes legais para celebração de contrato de prestação de serviço.

Além disso, podem ser considerados críticos sob a perspectiva da proteção de dados os processos que envolvem o tratamento de dados pessoais de crianças e adolescentes, bem como os que envolvem a coleta de dados pessoais sensíveis (tais como a coleta de dados biométricos para ingresso nas dependências da empresa) e a tomada de decisão automatizada.

Quais os contratos internos de maior impacto de risco frente à LGPD?

Entendemos que os contratos de alto impacto de risco são aqueles em que os fluxos de dados pessoais: (i) tenham relação direta com o objeto principal do contrato; (ii) envolvam dados sensíveis ou especiais; (iii) contemplem volume relevante de dados pessoais; e (iv) ocorram de forma continuada (as partes compartilham dados pessoais constantemente). Podem ser citados, por exemplo, os contratos de trabalho e os contratos de estágio que são celebrados com os colaboradores das empresas.

Nos contratos celebrados com os prestadores e/ou fornecedores de serviços, recomendamos revisão prioritária com a adoção de cláusula-padrão de proteção de dados robusta que seja

capaz de definir as responsabilidades de cada uma das partes, com especial atenção à Seção III da LGPD, que define a responsabilidade dos agentes e hipóteses de ressarcimento de danos aos titulares.

Quais seriam as fases mais imprescindíveis para aumentar a governança em LGPD?

Para a garantia das boas práticas de governança, é necessária a implementação de Programa de Governança em Privacidade (PGP), que consiste em um conjunto de mecanismos internos que garantam, em suma, o cumprimento dos padrões técnicos e legais e dos procedimentos internos para tratamento de dados pessoais, bem como a mitigação de riscos e o controle e a remediação de incidentes.

O Programa é constituído por três etapas: (i) iniciação e planejamento, em que se deve, em suma, definir o encarregado e o setor responsável pelo gerenciamento do PGP, mapear o estágio de adequação da empresa à LGPD e os riscos a serem mitigados, alinhar as expectativas da alta administração; (ii) construção e execução, em que deverão ser implementadas as políticas e as práticas para a proteção de dados, assim como elaborar o Relatório de Impacto à Proteção de Dados Pessoais, criar Política de Privacidade e Política de Segurança da Informação e promover a adequação de contratos e termos de uso; e (iii) monitoramento, em que se deve acompanhar indicadores de performance, gerir incidentes e realizar análise de resultados, assegurando a manutenção e o aperfeiçoamento do PCP, assim como sua efetividade.

Quais seriam as empresas no Brasil com maior solidez e maturidade em matéria de LGPD?

No Brasil, ainda é baixo o nível de maturidade das empresas em proteção de dados. Empresas multinacionais com estabelecimentos no Brasil, especialmente as que já se encontravam comprometidas com o cumprimento das obrigações da GDPR (*General Data Protection Regulation*) na União Europeia, saíram na frente no processo de adequação à LGPD.

Ademais, considerando que a ANPD foi formalmente constituída no ano de 2020, espera-se que a autoridade nacional ainda publique mais orientações sobre os dispositivos da lei. Deste modo, não se pode afirmar com precisão quais seriam as empresas no Brasil com maior solidez e maturidade em matéria de LGPD.

TRATAMENTO DE DADOS E INFORMAÇÕES

Anunciar os "aniversariantes do mês" em nossos meios de comunicação fere a LGPD?

Esse tratamento deverá ser feito conforme os requisitos da lei, tal como observando a base legal adequada e garantindo a transparência ao colaborador sobre o uso desta informação para essa finalidade.

Como se dará o tratamento dos dados divulgados via comunicação por aplicativo de telefone celular (Telegram e WhatsApp)?

O uso de aplicativos de telefone celular (como Telegram e WhatsApp) deverá ser avaliado sob a ótica dos requisitos da LGPD. A utilização desses aplicativos para compartilhamento de comunicação que possa conter dados pessoais pode colocar em risco a segurança dos dados, além de criar para a empresa um ônus em relação à responsabilidade sobre as informações compartilhadas na referida ferramenta.

É recomendada revisão do processo para confirmar se é de interesse da empresa manter a utilização dos referidos aplicativos para veiculação de informações que possam conter dados pessoais.

Em caso positivo, devem ser estabelecidas diretrizes internas a serem amplamente divulgadas sobre como os colaboradores devem utilizar a ferramenta para compartilhar dados, bem como a definição da plataforma oficial de comunicação e colaboração da empresa a fim de facilitar a adoção de medidas de governança.

Além disso, é recomendável o uso preferencial por aparelhos de celular da própria empresa e a necessidade do uso dessa ferramenta, devendo ainda, verificar o quanto é essencial seu uso para execução dos serviços.

Como ocorrerá o tratamento de dados no âmbito da empresa? Será realizado um *data mapping*?

A LGPD estabelece que o controlador poderá implementar programa de governança em privacidade que seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta e que seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados, conforme o Artigo 50, §2º, I, da LGPD.

Com o objetivo de definir o conjunto de dados pessoais da empresa e suas especificidades, é entendida como essencial a realização do mapeamento de dados/*data mapping*. Dessa forma, a empresa vai obter a visão geral inicial de seus dados, entender em que estágio se encontra em termos de adequação às normas da LGPD e o que deve ser ajustado e tratado.

A partir desse diagnóstico inicial, a empresa vai identificar e atuar nos dados que necessitam ser tratados, o local e a forma de armazenamento e compartilhamento, e a base legal.

CONSCIENTIZAÇÃO E CONTROLE DA LGPD

A empresa fará treinamento de conscientização dos seus funcionários sobre a LGPD?

A LGPD estabelece que o controlador poderá implementar programa de governança em privacidade que demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

É recomendado que as empresas realizem comunicações, treinamentos e capacitação dos seus colaboradores sobre o tema, para que eles sejam capazes de executar suas tarefas em conformidade com a LGPD.

Todos os empregados deverão entender, entre outras coisas:

- O que é a LGPD;
- Papéis e responsabilidades dentro da empresa;
- O que são dados, procedimentos internos de como usá-los, armazená-los e compartilhá-los;
- Riscos e consequências da não conformidade.

| Papéis e responsabilidades:

Qual a área da empresa mais comum para absorver e controlar a implementação das medidas necessárias pela LGPD?

A área responsável pela implementação da LGPD deve ser definida pela empresa considerando sua estrutura e necessidades. Em geral, há envolvimento dos setores Jurídico, Tecnologia e Ética e *Compliance*.

Vale destacar que algumas empresas optam por criar área específica para tratar de Proteção de Dados ou um Comitê de Privacidade dedicado.

Por fim, é importante a participação e suporte da alta gestão da empresa no processo de adequação e monitoramento do cumprimento da LGPD.

Quais as providências que as empresas devem adotar em relação aos dados pessoais que já estavam em seu poder antes da vigência da LGPD?

Dados armazenados na empresa devem ser identificados, avaliados e adequados à luz da LGPD. Isso faz parte do processo de mapeamento de dados/*data mapping*, mencionado anteriormente, com posterior tratamento dos dados.

A adequação da documentação interna pode incluir ajuste de cláusulas de contratos com terceiros e termos de consentimento, por exemplo, entre outros.

Quais os cuidados que as empresas devem observar em relação ao recebimento de dados pessoais obtidos em processos seletivos? Se o titular do dado não for contratado, é necessário pedir o seu consentimento e informar quanto tempo vai manter o armazenamento dos seus dados em seu banco de talentos?

Dados pessoais coletados de candidatos em processos seletivos devem ser tratados em conformidade com a LGPD.

Visando à transparência com os candidatos, é indicado que seja solicitado o consentimento e seja disponibilizada política de privacidade destinada aos candidatos em processos seletivos da empresa.

| Quanto à coleta de dados:

- É necessário indicar as bases legais para a coleta, sendo elas consentimento ou legítimo interesse;

- Deve haver transparência com os candidatos sobre a finalidade da coleta das informações que devem ser apenas as necessárias, relevantes e não discriminatórias;

- A não exigência do consentimento nesses casos não exime a empresa da obrigação de informar de forma transparente o candidato sobre a coleta de seus dados.

Quanto ao armazenamento de dados dos candidatos não contratados:

- Caso a empresa tenha interesse em manter os dados coletados do candidato não selecionado no banco de dados, é necessário pedir consentimento dele;

- A empresa também deverá informar o prazo de armazenamento das informações e garantir que elas serão descartadas após o período indicado.

Qual o papel do RH na implementação da política de LGPD?

A área de recursos humanos trabalha com grande volume de dados pessoais de seus colaboradores, portanto deve necessariamente se adequar à LGPD, observando seus princípios para coleta, compartilhamento, local e tempo de armazenamento desses dados.

Além de atuar com informações de candidatos, como mencionado anteriormente, o RH é responsável pela admissão e desligamento de empregados, processos relacionados a afastamentos, folha de pagamento, entre outros, e deve entender e reconhecer a sensibilidade desses dados.

Por fim, o RH também é responsável por compartilhar dados pessoais internamente com outras áreas da empresa. Para isso, deverá estar atento e limitar esse compartilhamento considerando sua necessidade e finalidade, além de garantir o correto tratamento e armazenamento dos dados.

OS TRÊS INTERLOCUTORES

Defina os papéis e responsabilidades de cada interlocutor:

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. É o agente de tratamento responsável por determinar as finalidades para as quais serão utilizados os dados pessoais coletados. Podem ser identificados como controladoras, por exemplo, as companhias que tratam os dados pessoais de seus colaboradores. O controlador é o responsável por garantir que os dados estão sendo tratados de acordo com as determinações da lei. O controlador pode ser responsabilizado pelos danos patrimoniais, morais, individuais ou coletivo como violações à legislação.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. É o agente de tratamento que trata dados pessoais para a finalidade exclusiva de cumprir com as orientações do controlador. Assim, o operador deverá tratar os dados pessoais conforme orientado pelo controlador e também responde pelos danos patrimoniais, morais, individuais ou coletivos, como violações à legislação (dever de reparação) – assim como o controlador. Responde solidariamente caso descumpra a legislação quando não tiver seguido as instruções lícitas do controlador (equipara-se ao controlador).

Encarregado: também chamado de DPO (*Data Protection Officer*), em virtude da nomenclatura do GDPR, é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (Autoridade Nacional de Proteção de Dados). Deve possuir independência para o exercício de suas funções, bem como um canal direto com o mais alto nível da estrutura interna para reportar.

Quais são as atualizações, principais discussões, obrigações e direitos sobre a figura de cada interlocutor acima?

Controlador: deve seguir o disposto na LGPD, devendo realizar o tratamento de acordo com os princípios ou orientar corretamente o operador, para que este realize um tratamento lícito. O controlador responde por danos patrimoniais, morais, individuais ou coletivos, como violações à legislação. Ainda responde de forma solidariamente pelos danos causados pelo operador, se diretamente envolvido no tratamento que resultar em danos.

Operador: deve seguir as diretrizes trazidas pelo controlador e tratar os dados de acordo com as políticas de privacidade referentes ao ordenamento jurídico.

Responde pelos danos patrimoniais, morais, individuais ou coletivos, como violações à legislação, assim como o controlador. Responde solidariamente caso descumpra a legislação, equiparando-se a este, caso não tenha seguido as suas instruções.

Encarregado: tem como responsabilidade legal estabelecer comunicação com os titulares e a Autoridade Nacional (ANPD), prestando esclarecimentos, providências e orientações internas.

Na LGPD, pelo menos por enquanto, o encarregado deve ser indicado pelo controlador, não havendo previsão expressa de indicação por parte do Operador.

Ainda que o encarregado seja uma figura que ganhou lugar nos holofotes em ambas as legislações (LGPD e GPDR, na Europa), é importante lembrar: em momento algum, há previsão sobre essa figura responder legalmente – entende-se, portanto, que cabe ao Controlador a sua fiscalização, que pode ser seu funcionário ou prestador de serviços por meio contratual, pois a quem interessa se o encarregado está desenvolvendo as suas atividades adequadamente é a própria empresa que o contratou. A responsabilidade, em caso de incidente, é do Controlador ou Operador (a depender do caso concreto), mas jamais do DPO/encarregado.

Observação: um ponto de discussão que pode ser suscitado no que concerne ao fato de a LGPD não ter, até o momento, mencionado hipóteses em que não é necessária a nomeação de um DPO. Na GDPR, existem exceções a essa obrigação quando as empresas podem ser qualificadas como de pequeno porte. É esperado que a ANPD regule esse aspecto da legislação em momento posterior. No entanto, até agora, a obrigação de nomear um DPO se aplica a todos os controladores. Há ainda discussão acerca da existência de conflito de interesse quando o DPO nomeado for colaborador da empresa. No âmbito de aplicação da GDPR, não é possível que o DPO seja um colaborador da empresa, pois ele deve estar livre de conflitos de interesse e não pode influenciar o uso de dados pessoais dentro da empresa.

Qual o fundamento para que as empresas de energia precisem contratar o(s) interlocutor(es) acima? É possível nomear alguém internamente?

Empresas de energia devem nomear um encarregado, conforme o Artigo 41 da LGPD, visto que até o momento não há na legislação nenhuma exceção que isente certas companhias da obrigação de possuir um DPO. As empresas de energia são, elementarmente, controladoras dos dados pessoais de seus próprios colaboradores e, portanto, tratam dados pessoais em suas atividades e estão sujeitas às determinações da LGPD.

Não há qualquer impedimento atual para que a nomeação de um DPO seja feita internamente (algum colaborador do Jurídico ou TI, por exemplo). Contudo, vale ressaltar a possibilidade de ser suscitado um possível conflito de interesses nesses casos.

Quais são as implicações e penalizações de não contratar/nomear o(s) interlocutor(es) acima?

A empresa será considerada não adequada aos ditames da LGPD, podendo sofrer sanções administrativas da ANPD, penalizações da Aneel, bem como perda da sua credibilidade junto ao mercado.

Conforme na questão anterior, a indicação de um encarregado é obrigação prevista pela LGPD. Dessa forma, caso não atendida, poderá ensejar o risco da aplicação das multas previstas pelo Artigo 52 da lei, que inclui desde uma advertência, com indicação de prazo para adoção de medidas corretivas, até multa de até 2% do faturamento da empresa (limitada a 50 milhões de reais). As sanções serão aplicadas apenas a partir de agosto de 2021 e após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto.

Os controladores estão obrigados a realizar o Relatório de Impacto à Proteção de Dados Pessoais para cada tratamento de dados? Se sim, qual a periodicidade? Há algum modelo?

De acordo com o Artigo 10, § 3º, da LGPD, a ANPD poderá solicitar ao controlador Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando o tratamento tiver como fundamento seu interesse legítimo. Além disso, de acordo com o Artigo 38, a ANPD poderá determinar ao controlador que elabore o relatório, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados sempre os segredos comercial e industrial. Não há modelo definido ou previsão expressa na LGPD quanto ao conteúdo do relatório, com a especificação taxativa de todos os elementos que devem compor o documento, ou mesmo em quais situações a sua elaboração será imprescindível ou até mesmo dispensável, cabendo à Autoridade Nacional regulamentar essas questões no futuro. No entanto, a LGPD estabelece que o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Sendo assim, o RIPD não é um documento a ser elaborado periodicamente em todas as situações. Como uma prática de governança, é recomendável que empresas elaborem o RIPD sempre que o tratamento puder ensejar alto risco para o titular de dados, por exemplo, quando está sendo tratada uma grande quantidade de dados pessoais ou dados pessoais sensíveis.

Quais os cuidados e formalidades que devem ser adotados no caso de compartilhamento de dados entre controladores independentes?

Para que haja compartilhamento de dados entre controladores independentes, é preciso que a empresa cumpra com as obrigações de transparência perante o titular de dados sobre a possibilidade de compartilhamento, formalizando o seu consentimento, além de garantir que os devidos cuidados estão sendo tomados para proteção dos dados de acordo com as determinações da lei.

É recomendável que as partes estabeleçam os limites de suas obrigações através de cláusulas e adendos apropriados para proteção do tratamento de dados pessoais realizados por esses controladores independentes. A LGPD não define esse cenário nem mesmo prevê contratos específicos para regular um controle conjunto de controladores de dados.

Qual a recomendação nas situações em que o tratamento de dados está sujeito ao controle de dois controladores independentes? Há contratos específicos para regular o controle conjunto?

Embora a LGPD não explicite o conceito de controladoria conjunta, é possível inferir que ele está contemplado no sistema jurídico de proteção de dados. A definição das funções dos controladores conjuntos implica consequências no que diz respeito às funções dos agentes de tratamento e aos direitos dos titulares. Para o regulamento europeu, a controladoria conjunta ocorre quando há "participação conjunta" na determinação de "finalidades e meios de tratamento". Conforme o Comitê Europeu de Proteção de Dados ("EDPB"), a finalidade do tratamento pode ocorrer a partir de decisões comuns ou convergentes.

Entretanto, ainda que o mesmo conjunto de dados seja tratado, não haverá controladoria conjunta se os objetivos do tratamento forem distintos. Se estas finalidades não forem comuns, convergentes ou complementares, ambos serão controladores singulares em relação ao tratamento de dados e a controladoria conjunta não estará estabelecida, o que afastaria a incidência do Artigo 42, §1º, II, da LGPD. Segundo o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, publicado pela ANPD, em maio de 2021, ao adaptar a concepção europeia para o cenário da LGPD, pode-se entender o conceito de controladoria conjunta como "a determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD".

É importante frisar que controladores conjuntos são igualmente responsáveis por danos causados aos titulares de dados e, portanto, estão conjuntamente sujeitos às sanções previstas na lei. Até o momento, não foram estabelecidas obrigações de firmar contratos específicos nessas situações.

LEGITIMAÇÃO E BASES LEGAIS

Nas relações de trabalho, quais são as hipóteses que vão legitimar o tratamento de dados pessoais de forma mais recorrente?

As bases legais usuais que podem legitimar o tratamento de dados originado por relação de trabalho são (i) cumprimento de obrigação legal ou regulatória, (ii) execução de contrato ou de procedimentos preliminares relacionados ao contrato; e (iii) exercício regular de direitos em processo judicial, administrativo ou arbitral.

A título exemplificativo, atividades como recrutamento de novos colaboradores e admissão desses recrutados podem ser legitimadas pelo legítimo interesse legal do controlador, ao passo que atividades como coleta de dados para geração da folha de pagamento podem ser justificadas pela execução de contrato.

O consentimento do colaborador será necessário em determinados fluxos de processamento, mas seu uso em geral não é recomendável como base legal adequada em virtude da relação de subordinação entre as partes, que poderá impactar na liberdade do titular em anuir ou não com determinado tratamento de seus dados pessoais.

A LGPD estabeleceu hipóteses de bases legais que podem ser utilizadas no lugar do consentimento expresso do titular para a coleta e tratamento de dados pessoais. Uma dessas hipóteses é o legítimo interesse do controlador. Operações do cotidiano das empresas (exs.: outorga de procurações, dados indicados em contratos comerciais etc.) que sejam realizadas com base no interesse legítimo podem ser registradas em protocolos genéricos da empresa (ex.: políticas internas que estabeleçam que todo tratamento realizado para fins de outorga de procuração poderá ser com base no interesse legítimo)?

O legítimo interesse do controlador pode ser utilizado em substituição ao expresso consentimento do titular nos casos em que se destinem a finalidades legítimas, como o apoio e a promoção das atividades do controlador e a proteção do exercício de direitos pelo titular. No primeiro caso, somente os dados pessoais estritamente necessários poderão ser tratados.

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 dessa 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.

Pode-se indicar o legítimo interesse quando: (i) há uma situação real e concreta para o tratamento de dados; (ii) o tratamento tem como objetivo apoio e promoção das atividades do controlador; (iii) a atividade tem impacto mínimo na privacidade dos titulares; (iv) os dados pessoais são coletados de forma proporcional; e (v) há a garantia ao titular de transparência em relação a como seus dados pessoais serão tratados. Sendo assim, é possível que operações do cotidiano da empresa, como a outorga de procurações, sejam realizadas com base no legítimo interesse do controlador. Esse tratamento, para fins de transparência, poderá ser descrito em políticas internas de forma genérica desde que não haja prejuízo à transparência. Por outro lado, atividades como a coleta de dados para inserção em contratos comerciais podem ser justificadas pela base legal de execução de contrato ou procedimentos preliminares ao contrato.

EM CASO DE IRREGULARIDADES OU DESLIGAMENTO

A empresa deve manter os dados pessoais dos empregados após o seu desligamento? E se o empregado solicitar a eliminação desse dado?

A empresa deverá manter os dados para eventual cumprimento de obrigação legal (cumprimento de legislação trabalhista), ainda que o empregado solicite a sua eliminação, conforme dispõe o Artigo 16 da lei. Admitindo a possibilidade de um ex-empregado ingressar com reclamação trabalhista, a empresa, para exercer seu direito de defesa, precisa estar de posse daquelas informações e de documentos necessários ao deslinde da causa. O que ela não pode é divulgar as informações para terceiros.

Em caso de irregularidades no tratamento e coleta de dados pela empresa, quem vai ser responsabilizado? Existem penalidades para isso?

Caso incorram no descumprimento da legislação, poderão ser responsabilizados, individual e solidariamente, o operador e o controlador, sejam eles pessoas naturais ou jurídicas.

De acordo com o Artigo 52 da LGPD, o agente de tratamento que cometer infrações à legislação estará sujeito à: (i) advertência; (ii) multa de até 2% do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil, limitada a 50 milhões de reais por infração; (iii) multa diária, observado o mesmo limite; (iv) publicização da infração; (v) bloqueio e/ou eliminação dos dados pessoais relacionados à infração; (vi) suspensão de funcionamento de banco de dados da atividade de tratamento de dados pelo período máximo de 6 meses, prorrogável por igual período; e, (vii) proibição total ou parcial do exercício de atividades de tratamento de dados.

As diretrizes para a dosimetria da multa serão definidas pela ANPD.

Em caso de irregularidades praticadas por empregados ou prestadores de serviços, como o compartilhamento de informações sigilosas da empresa, há possibilidade de eles serem responsabilizados, nos termos da LGPD? Existe algum outro tipo de penalidade?

A LGPD tem como finalidade a proteção dos "direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Diante do cenário descrito (compartilhamento de informações sigilosas da empresa que envolvem dados pessoais), não seria possível a responsabilização de empregados ou prestadores de serviços (pessoa física) nos termos da LGPD. No entanto, seria possível buscar a responsabilização civil dos empregados ou prestadores de serviços em outras esferas, podendo sofrer dispensa por justa causa (amparada no Artigo 482, alínea g, da CLT), responder por algum tipo de reparação civil, e até mesmo criminal, a depender da conduta praticada.

DIRETORIA EXECUTIVA

Presidente
Roberto Ardenghy

Diretora Executiva Corporativa
Fernanda Delgado

Gerência de Recursos Humanos
Sandra Martinez

Gerência de Comissões e Gestão do Conhecimento
Lisandro Gaertner

Comissão de Gestão de Pessoas
Ana Martins de Andrade - Shell
Cilene Viana - American Bureau of Shipping
(ABS) Elaine de Souto - Ecopetrol Brasil
Flavia Cavalcanti - Enauta
Iane Moreira - Ocyan
Ilana Oliveira - Saipem
Renato Peregrina - Galp

EXPEDIENTE

Gerente de Comunicação e Relacionamento com Associados
Tatiana Campos

Revisão de Conteúdo:
Tatiana Campos

Projeto Gráfico
Erick Vianna

Banco de Imagens
IBP

INSTITUTO BRASILEIRO DE PETRÓLEO E GÁS

/ibpbr @ibp_br /ibpbr /IBPbr @ibp_br

IBP - Instituto Brasileiro de Petróleo e Gás
Av. Almirante Barroso, 52 - 21º e 26º andares - RJ Tel.: (21) 2112-9000 - ibp.org.br
relacionamento@ibp.org.br