DESCOMPLICANDO A LGPD

Dr. Fabricio Vieira Camacho

Sua empresa se enquadra em algum destes modelos de atuação?

- Comercializa produtos e/ou serviços para pessoas físicas.
- Possui funcionários em regime de contratação CLT.
- Presta serviços de mão-de-obra terceirizada em regime de CLT para outras empresas.
- Realiza tratamento de dados pessoais na execução de suas atividades à outras empresas.
- É entidade sem fins lucrativos que oferece produtos/serviços, mesmo que gratuitos à PF.
- Realizou ou está em adequação da LGPD, mas tem dúvidas se realmente estará compliance.
- Seu negócio está sujeito a risco de descumprimento da LGPD e ser denunciado.

NÓS TEMOS A SOLUÇÃO

A Quattro Consultoria possui parceria com uma empresa especializada em Direito Digital, Privacidade & Proteção de Dados, consultoria às áreas jurídica e TI, e fornece também contrato permanente de DPO (Data Protector Officer).

Nossas serviços visam o compliance integral e mitigação do risco da aplicação de multas que poderão chegar a R$ 50 milhões, não só no caso de vazamento de dados pessoais ou uso indevido, mas também o risco da empresa não estar compliance e ser autuada mediante denúncia ou fiscalização federal aleatória.

4UATTRO

Quattro Consultoria em TI
Telefone: (11) 4081-1110 I (11) 9-9644-5157
E-mail: lgpd@4uattro.com.br

www.4uattro.com.br

Descomplicando a LGPD

Lei Geral de Proteção de Dados

Dr. Fabricio Vieira Camacho

DPO (Data Protection Officer)/Compliance Officer, advogado, palestrante e consultor especializado em Proteção de Dados, Anticorrupção e Prevenção à Lavagem de Dinheiro, cofundador da Associação Nacional de Proteção de Dados – Brasília (DF), presidente da Comissão de Direito Digital, Privacidade & Proteção de Dados – OAB Barueri (SP), experiência de 23 anos em Tecnologia, Segurança, Gestão de Riscos, Projetos, Compliance e Perícia Tecnológica.

Linkedin: www.linkedin.com/in/fvcamacho

SUMÁRIO

Desde agosto de 2018, há uma crescente demanda por informações relativas à LGPD (Lei Geral de Proteção de Dados), e consequentemente, tenho sido consultado para realizar a orientação necessária ao correto entendimento e abrangência da Lei, identificar o risco ao negócio, e por fim, garantir a mitigação do risco empresarial através da condução e suporte de programa de implantação da LGPD.

Aproveito esta oportunidade de espaço para abordar, através de uma linguagem menos técnica e de forma breve, as iniciais e frequentes questões sobre a LGPD, contribuindo então para que o sócio empresário tenha uma visão geral sobre o tema e consequentemente possa decidir com mais clareza a forma na qual o assunto será abordado em sua organização.

Então, dando sequência, passo a responder as mencionadas questões.

Dr. Fabricio Vieira Camacho

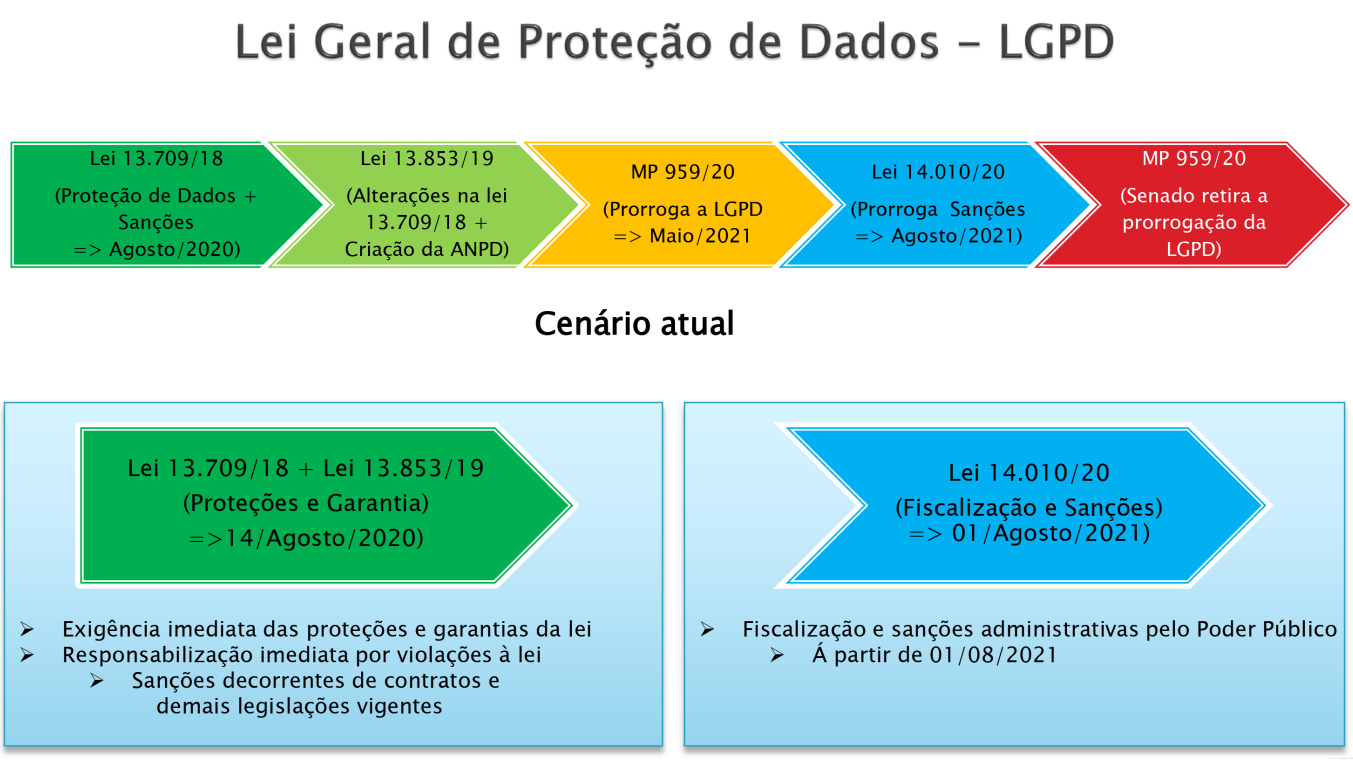
O que é exatamente a LGPD?

A LGPD – Lei Geral de Proteção de Dados, foi criada pelo ex-presidente Michel Temer, através da Lei 13.709 em 14 de agosto de 2018, posteriormente alterada pela Medida Provisória – MP 869/2018 e atualmente com novas disposições trazidas pela Lei 13.853 de 8 de julho de 2019, sendo as recentes na gestão atual do Presidente Jair Messias Bolsonaro.

A lei considerou em sua publicação que entraria imediatamente em vigor nos aspectos relacionados à ANPD e para o restante da lei entraria em vigor em 24 (vinte e quatro) meses após sua publicação, ou seja, a lei passa a vigorar totalmente em 17 de agosto de 2020.

No final de abril de 2020, o Governo Federal por força da Medida Provisória – MP 959/2020 determinou novo prazo para vigência da lei, o que de fato postergou a eficácia e exigência da LGPD para 03 de Maio de 2020.

Logo em seguida, em junho de 2020, é sancionada a Lei 14.010/2020, que embora tratasse de assuntos emergenciais e transitórios nas relações jurídicas no período de pandemia do COVID-19, estabeleceu em seu artigo 20º que o processo de fiscalização e sanções administrativas só poderão ocorrer à partir de 1º de agosto de 2021.



Neste contexto, a Medida Provisória – MP 959/2020 teve seu curso e o Senado Federal retirou do texto o artigo que prorrogava a exigência da LGPD, retornando então a obrigatoriedade para agosto de 2020 e o respectivo Projeto de Lei de Conversão seguiu para sanção do Presidente da República.

Portanto, no cenário atual temos a seguinte situação, a LGPD passa a ser exigida a partir de agosto de 2020 e eventuais fiscalizações e sanções administrativas só poderão ocorrer a partir de agosto de 2021.

Objetivo da Lei

De forma também resumida, o objetivo da Lei é de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, fundamentalmente sobre o respeito à privacidade, inviolabilidade da intimidade / honra / imagem, liberdade de expressão, etc., em razão das operações de coleta e tratamento realizadas por pessoas físicas ou jurídicas em território nacional ou para ofertas de bens e serviços de indivíduos localizados em território nacional.

A quem a lei se destina

Assim como indicado no parágrafo anterior, reforço que esta lei é aplicável às pessoas naturais (PF - pessoa física) ou PJ - pessoa jurídica de direito público e privado, desde que realizem o tratamento de dados pessoais.

Apenas para facilitar, destaco alguns conceitos relevantes as PJ - pessoas jurídicas:

- direito privado: aquelas de iniciativa e composta por particulares, sendo as associações, as sociedades, as fundações, as organizações religiosas, os partidos políticos, as ONG´s e as empresas individuais de responsabilidade limitada, etc.
- direito público interno, se dividem em entes de administração direta: União, Estados, Distrito Federal, Territórios e Municípios; e entes de administração indireta, como é o caso das autarquias (como o INSS) e das demais entidades de caráter público criadas por lei.

Com isso, ressalto que até o momento não há qualquer previsão legal que exclua a necessidade de adequação para empresas em razão do porte, faturamento, número de funcionários, quantidade de operações, etc. Portanto,

bastando o simples fato de realizar o tratamento de dados com sendo suficiente à aplicação da LGPD.

Conceitos de tratamento, dados pessoais, titular e agentes de tratamento

Neste contexto, se faz necessária a compreensão de alguns conceitos complementares para confirmar se o agente (PF ou PJ) realmente executa uma ação relacionada e consequentemente está sujeito a aplicação da LGPD, além de já esclarecer o papel e importância de partes envolvidas:

- tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- dados pessoais: toda e qualquer informação relacionada a pessoa natural (PF) identificada ou identificável. (Exs.: nome completo, endereço de residência, e-mail, número de documentos pessoais – RG, CPF, CNH, placa do carro, IP, sinal de wi-fi).
- dados pessoais sensíveis: dado genético/biométrico, origem racial/étnica, convicção religiosa, opinião política, filiação a sindicato, etc..).
- titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- encarregado de dados ou DPO (data protection officer): 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).

Observações e requisitos com o tratamento de dados pessoais

Também decorre de lei que o tratamento de dados pessoais deve sempre observar a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não

discriminação, responsabilização e a prestação de contas.

Neste mesmo sentido, o tratamento só pode ser realizado nas hipóteses de: consentimento pelo titular, cumprimento de obrigação legal ou regulatória, necessária execução de contrato, proteção da vida ou incolumidade física do titular/terceiro ou proteção de crédito.

Direitos dos titulares dos dados pessoais

Não há dúvida a importância de conhecer os direitos dos titulares, uma vez que o controlador tem a obrigação legal em garanti-los a qualquer momento e mediante requisição pessoal ou de seu representante:

- direitos dos titulares: confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados, portabilidade dos dados a outro fornecedor de serviço ou produto, eliminação dos dados pessoais, informação sobre consequências da negativa de consentimento, revogação do consentimento e ainda de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

Função do Encarregado de Dados / DPO (Data Protection Officer)

Neste tocante, a LGPD também seguindo padrões semelhantes de leis internacionais, principalmente a europeia (EU 2016/679 – GDPR General Data Protection Regulation), determinou a necessidade do controlador em indicar o encarregado responsável pelo tratamento de dados, bem como as informações de contato de forma pública, de preferência no site da empresa.

Na mencionada lei europeia, o encarregado de dados recebe o nome de DPO (Data Protection Officer) e executa funções similares.

O Encarregado de Dados / DPO (Data Protection Officer), é responsável por:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.
- receber comunicações da autoridade nacional (ANPD) e adotar providências;
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

4UATTRO

TECNOLOGIA DE PONTA
AO SEU ALCANCE

A QUATTRO Consultoria em TI é formada por profissionais com mais de 20 anos de experiência no setor de TI, oferecemos soluções completas que reúnem produtos e serviços, alinhadas com as características e necessidades de negócio dos nossos clientes.

Atuando como integradora de soluções, a QUATTRO possui um ecossistema de parcerias com os melhores fornecedores de tecnologia do mercado, além de serviços com profissionais certificados, metodologias, gestão de projeto e base de conhecimento para atuar em diversas áreas de negócios.

Quattro Consultoria em TI
Telefone: (11) 4081-1110 I (11) 9-9644-5157
E-mail: lgpd@4uattro.com.br
https://www.linkedin.com/company/4uattro
www.4uattro.com.br

- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Importante esclarecer que o Encarregado de Dados / DPO (Data Protection Officer) é um profissional, que pode ser funcionário da empresa (contratação em regime CLT) ou até mesmo um prestador de serviço (contratação de PJ).

Entretanto, este profissional ou prestador de serviço, precisa ter um amplo conhecimento certificado capaz, não só de cumprir com excelência as funções descritas acima, mas de garantir uma completa e integral adequação organizacional nos âmbitos tecnológico, organizacional e jurídico da empresa, identificando e aprimorando o ecossistema na medida em que ocorre a mudança da tecnologia e na organização / das boas práticas de segurança e governança / da legislação ao longo do tempo.

Responsabilidade e ressarcimento de danos

No que tange a responsabilidade e ressarcimento por danos causados, inicialmente esclareço que, embora estejamos analisando uma lei específica (LGPD), a empresa deverá ter uma visão ampla de proteção quando estiver realizando sua adequação a esta norma, inclusive sob o aspecto de produção futura de provas, pois em uma situação de litígio, todas as partes envolvidas, podem e devem se utilizar de todo o arcabouço jurídico, ou seja, demais leis vigentes, para fundamentar o direito pretendido na busca de sua tutela jurisdicional.

Passa a ficar mais clara essa visão, ressalto que:

- o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
- o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador.
- os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente.
- o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados.
- aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

- os agentes de tratamento só não serão responsabilizados quando provarem:

¤ que não realizaram o tratamento de dados pessoais que lhes é atribuído;

¤ que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

¤ que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Segurança e Governança em matéria de proteção de dados

É evidente, e assim consta na lei que, 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.

Essas medidas de segurança devem ser consideradas desde a fase de concepção do produto ou serviço (conhecida também como by-design) até a sua execução. Além disso, é necessário que a organização passe a tratar essas boas práticas como uma nova forma padrão ao produzir novos produtos e serviços (conhecida também como by-default).

Isso quer dizer que, todo o ecossistema utilizado para o tratamento de dados pessoais deve ser estruturado de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Ainda, de acordo com a estrutura, a escala, e o volume de suas operações, bem como da sensibilidade dos dados em relação a probabilidade e a gravidade dos danos, 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;
- seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

- estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- conte com planos de resposta a incidentes e remediação; e
- seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
- demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

Por fim, não resta dúvida ainda que todo esse conjunto de boas práticas envolvendo segurança e governança devem ser atualizados com a frequência necessária, de forma a se manterem eficazes ao longo do tempo.

Comunicação em caso de incidentes

É de responsabilidade do controlador, o que muitas vezes é a função do Encarregado de Dados / DPO (Data Protection Officer), comunicar à autoridade nacional (ANPD) e ao titular, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Neste caso, a autoridade (ANPD) verificará e poderá, dependendo da gravidade do incidente, determinar que o controlador realize a ampla divulgação em meios de comunicação e adote medidas para conter ou mitigar os efeitos do incidente.

Na verificação da gravidade do incidente é levada em consideração a comprovação de adoção das medidas técnicas necessárias.

Fiscalização, Sanções e Atenuantes previstos na lei

Os agentes de tratamento, ou seja, Controlador e Operador, em razão das

infrações, ficam sujeitos a sanções administrativas aplicáveis pela autoridade nacional (ANPD), sendo:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total a que se refere o item acima;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Importante ressaltar que, as sanções ocorrerão em processo administrativo, respeitando a ampla defesa, e ainda considerarão os seguintes critérios:

- a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- a boa-fé do infrator;
- a vantagem auferida ou pretendida pelo infrator;
- a condição econômica do infrator;
- a reincidência;
- o grau do dano;
- a cooperação do infrator;
- a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e

adequado de dados;

- a adoção de política de boas práticas e governança;
- a pronta adoção de medidas corretivas; e
- a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

ANPD – Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão da administração pública federal, integrante da Presidência da República, com poder de autonomia e decisão.

A ANPD é composta de:

- Conselho Diretor, órgão máximo de direção;
- Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
- Corregedoria;
- Ouvidoria;
- órgão de assessoramento jurídico próprio; e
- unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente, e disporá sobre o regimento interno da ANPD.

Compete à ANPD:

- zelar pela proteção dos dados pessoais, nos termos da legislação;
- zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
- elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- apreciar petições de titular contra controlador após comprovada pelo

titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

- promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
- estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
- promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
- dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;
- solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
- elaborar relatórios de gestão anuais acerca de suas atividades;
- editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
- ouvir os agentes de tratamento e a sociedade em matérias de interesse

relevante e prestar contas sobre suas atividades e planejamento;

- arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;
- realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;
- celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;
- editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;
- garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento;
- deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;
- comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
- comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;
- articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e
- implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

O RH da empresa também será impactado pela LGPD?

Esse questionamento é recorrente das organizações, pois logo que se fala em proteção de dados, a maioria das pessoas e até mesmo de alguns profissionais, se equivocam ao limitar tal necessidade de proteção apenas aos dados de clientes que compraram seus produtos e serviços.

Entretanto, não há dúvida que os dados pessoais dos funcionários também são objeto de proteção e das mesmas garantias estabelecidas na LGPD, e muitas vezes, com ainda maior relevância, por serem de caráter sigiloso, muitas delas consideradas sensíveis e com alto grau de risco de dano ao titular em caso de um incidente.

Podemos utilizar como exemplo, a situação onde uma base de dados de funcionários contendo o nome completo, telefone e proventos mensais, é copiada integralmente e vendida para um terceiro oferecer seus serviços, ou pior ainda, essa base de dados é copiada e acaba na posse de uma quadrilha que passa a fazer ameaças ou outros tipos de crimes a esta pessoa e seus familiares.

Outro exemplo a se destacar, são as informações de funcionários relativas a sua sexualidade, religião, deficiências ocultas e até mesmo de eventuais doenças não transmissíveis, as quais uma vez publicizadas podem gerar um alto grau de risco ao titular, por atos discriminatórios ou até mesmo em razão de ameaça à sua vida por indivíduos ou grupos criminosos radicais de opiniões contrárias.

Sendo assim, o RH, considerando que está responsável pelo recrutamento, seleção e gestão do funcionário da admissão ao término da relação de emprego, deve considerar todas as precauções necessárias com estes dados, desde o recebimento do curriculum até a momento final em que os dados podem ser excluídos de sua base de dados, considerando ainda o prazo legal das normas aplicáveis.

Portanto, no contexto atual da LGPD, é fundamental que o RH (Recursos Humanos) participe da estratégia juntamente com o restante da organização no que se refere a garantia da privacidade e proteção de dados pessoais.

Quais os impactos à empresa, estando ou não de acordo com a LGPD?

Há um grande número de impactos a serem avaliados em diferentes cenários, dependendo principalmente do negócio específico da organização, e que merecem total atenção do empresário, mas para facilitar essa visão vamos destacar os principais impactos nos 3 cenários mais frequentes e discutidos, sendo:

1. Empresa implanta integralmente a LGPD e dentro do prazo legal;

- minimiza consideravelmente os riscos de sanções legais;
- demonstra a seus funcionários e clientes que se preocupa com a exposição dos dados pessoais que estão seu poder;
- se diferencia de outras empresas que não possuem tal preocupação;
- evita ou diminui consideravelmente os gastos futuros com defesas administrativas e/ou judiciais relacionadas a LGPD;
- empresa tem maior valor de mercado em caso de venda, pois gerencia e mitiga riscos empresariais;

2. Empresa implanta LGPD no prazo legal, mas não faz integralmente;

- minimiza parcialmente os riscos de sanções legais;
- fica sujeita a sanções por reincidência;
- demonstra a seus funcionários e clientes que se preocupa relativamente com a exposição dos dados pessoais que estão seu poder;
- se diferencia minimamente de outras empresas que não possuem tal preocupação;
- terá gastos futuros com defesas administrativas e/ou judiciais relacionadas a LGPD;
- empresa terá seu valor de mercado reduzido em caso de venda, pois não mitiga seus riscos empresariais completamente;

3. Empresa não implanta a LGPD no prazo legal;

- totalmente exposta aos riscos de sanções legais;
- demonstra a seus funcionários e clientes que NÃO se preocupa com even-

tual exposição dos dados pessoais que estão seu poder;

- se igualará no mercado a outras empresas que não possuem aderência à lei;
- terá gastos futuros com defesas administrativas e/ou judiciais relacionadas a LGPD;
- arcará financeiramente com prejuízos derivados de condenações administrativas e/ou judiciais relacionadas a LGPD;
- sofrerá uma exposição negativa de seu negócio em razão da publicidade das condenações;
- colocará em risco a continuidade da empresa em razão dos prejuízos financeiros;
- empresa terá seu valor de mercado extremamente reduzido em caso de venda, pois não mitiga seus riscos empresariais.

Quais são as ações a serem realizadas para estar compliance com a LGPD?

Pela experiência adquirida em mais de 20 anos realizando ações em diferentes empresas, incluindo gestão de riscos e compliance de normas nacionais e internacionais, destaco e apresento uma visão macro do que deve ser realizado para alcançar a integralidade de aderência à norma, entretanto, o detalhamento necessário seguirá de acordo com aspectos inerentes ao negócio, pois mesmo as empresas que atuam no mesmo segmento e ofertam os mesmos produtos e/ou serviços possuem diferentes aspectos que refletirão nas ações necessárias do programa de compliance.

Em uma visão macro, para facilitar o entendimento, o programa de compliance da LGPD deve considerar minimamente o atendimento das ações abaixo relacionadas:

- nomear o Encarregado de Dados / DPO (Data Protection Officer) para conduzir todo o processo de compliance;
- criar o Modelo de Governança de Privacidade & Proteção de Dados;
- executar o Due Diligence/Gap Analisys no âmbito da LGPD;
- elaborar o RIPD (Relatório de Impacto em Proteção de Dados);

- realizar o Plano de Conscientização;
- construir as medidas futuras de tratamento e gestão dos dados pessoais;
- considerar e implementar correções nos dados pessoais da base;
- promover a garantia dos direitos dos titulares;
- certificar a aderência de compliance a LGPD;
- realizar o PDCA para melhoria contínua.

Quanto tempo é necessário e quanto custará à empresa estar de acordo com a LGPD?

Por fim, informar o tempo e custo necessários para a implantação integral da LGPD em uma empresa só é possível após a realização do Due Diligence/Gap Analisys, ou seja, após um levantamento de aspectos específicos sobre o negócio e uma análise de sua relação com a previsão / alcance da LGPD e demais normas relacionadas, haverá a possibilidade de identificar claramente o quanto deverá ser aprofundado em cada etapa, além do respectivo esforço e consequentemente indicar o valor a ser gasto nesta necessária adequação.

Sincomavi

Soluções que Você e sua empresa precisam

SERVIÇOS ESSENCIAIS

O Sincomavi proporciona às empresas associadas uma série de serviços de grande valor, que de outra forma exigiria a contratação de consultores e escritórios especializados com grande desembolso.

Convenções Coletivas de Trabalho

Acordos Coletivos de Trabalho

Com equipe experiente e capacitada, a entidade consegue direcionar as demandas dos empresários do varejo e firmar CCTs e a ACTs de acordo com as necessidades da organização. São mais de trinta anos de experiência negociando com alguns dos principais sindicatos de empregados do País.

MAIS SERVIÇOS

- Recuperação de Tributos
- Assessoria Jurídica
- Câmara de Conciliação Trabalhista
- Certificado Digital
- Escola de Negócios
- Ensino a Distância (EAD)
- Comitês e Grupos de Trabalho
- Placas e Cartazes Obrigatórios
- Requerimentos e Declarações
- Manuais, cartilhas e e-books
- Convênios e Parceiras
- Marketing Digital

Mais informações

Telefone (11) 3488-8200 | sincomavi@sincomavi.org.br

SEJA UM ASSOCIADO SINCOMAVI