CARTILHA LGPD

prodam

CIDADE DE SÃO PAULO

Cidade de São Paulo
Bruno Covas - Prefeito

Secretaria de Inovação e Tecnologia (SMIT)
Juan Quirós - Secretário municipal

PRODAM - Empresa de Tecnologia da Cidade de São Paulo
Alexandre G. Amorim - Diretor-presidente
Jorge Pereira Leite - Diretor de Administração e Finanças
Alexandre Gedanken - Diretor de Desenvolvimento e Operações de Sistemas
Camila Cristina Murta - Diretora Jurídica
Alexandre Gedanken - Diretor de Infraestrutura e Tecnologia
Luciano Ferreira - Diretor de Participação
Paulo Cesar Goulart de Miranda - Diretor de Relacionamento Institucional e Mercado

EQUIPE TÉCNICA

Data Protection Officer - DPO
Camila Cristina Murta

Diretoria Jurídica (DJU)
Camila Cristina Murta
Márcio Rodrigues Pereira Mendes

Comitê LGPD
Wagner Kanagusuko (GIT)
Lucia Cristina Freire de Almeida e
Fabiana Silva Brito (GFH)
Jose Fumihiro Narasaki (GFA)
Sandra Mara T.M. Barreto (GPO)
Adriana Pereira de Oliveira Taborda e
Camila Cristina Murta (DJU)
Maria Aparecida L. S. Rocha,
Rubens Francisco de Souza Irrera
Ivan Borges Farhat, Carla Massae Toma e
Solange Cristina F. C. Campos (GPR)
Marcos Cesar da Costa (GRP)
Manoel Pacífico de São Félix e
Luciano de Azevedo Farias Ferreira (DIPAR)
Kleber do Prado de Carvalho (GDA)
Raquel Maria Sebastião de Moraes(GPR)

Comunicação e Marketing
Lucas Campagna Filho
Marcelo Pietragalla
Rebeca Tami Santana Osanai

MENSAGEM DO PRESIDENTE

A Prodam, na qualidade de integradora estratégica de soluções de tecnologia da informação e comunicação para a cidade de São Paulo disponibiliza, desde 1971, sistemas e soluções de tecnologia da informação, sustentação de infraestruturas, operações estratégicas e gestão de negócio, contribuindo para a melhoria da prestação do serviço público, bem como para promoção da transparência e ampliação da participação social.

O mundo está cada vez mais conectado, a velocidade e a quantidade de informações crescem exponencialmente. Estabelecer uma conexão entre o uso da tecnologia relacionada às boas práticas para a modernização da administração pública foi e seguirá como norte das nossas ações.

Vivemos a era da privacidade dos dados. Sabemos o quanto esta temática está no centro da agenda, com legislações e discussões que ganharam ainda mais impulso com o Regulamento Geral de Proteção de Dados, que no Brasil ganhou corpo com a publicação da Lei nº 13.709/2018, a nossa LGPD – Lei Geral de Proteção de Dados.

Mais do que uma lei, a LGPD possui no seu corpo princípios, fundamentos e ações que todas as pessoas, empresas e governos que tratem dados pessoais devem seguir, mas, principalmente, coloca o dono da informação como figura central: o titular dos dados é o foco.

E é, justamente, com esse foco, que a Prodam elaborou esta cartilha, como um direcionador à empresa e à gestão pública municipal, buscando trazer luz aos pontos fundamentais e esclarecimentos aos pontos mais complexos da lei.

A Prodam reforça o compromisso de se manter à frente nas gestões e atuando como referência no segmento de empresa de tecnologia.

Esta Cartilha é destinada a vocês, gestores e servidores públicos, que querem conhecer a Lei Geral de Proteção de Dados e contribuir para a sua aplicação.

Boa leitura!

Alexandre G. Amorim

MENSAGEM DO SECRETÁRIO

A Secretaria Municipal de Inovação e Tecnologia (SMIT), como ente responsável por incentivar, prospectar, desenvolver e implantar métodos, instrumentos e técnicas que conduzam à melhoria e inovação na organização e serviços prestados pela administração pública, utiliza recursos da tecnologia da informação e comunicação como forma de ampliar a qualidade do atendimento ao cidadão e promover sua participação no desenvolvimento de uma cidade inteligente.

Em um mundo cada vez mais ágil e conectado, fruto das transformações digitais decorrentes da última década, é fundamental estar atento aos debates sobre a necessidade de regulamentações que assegurem a privacidade e a proteção de dados pessoais.

Mais do que garantir conexões seguras, é importante analisar como se dá o tratamento e o armazenamento de informações de milhares de pessoas. É nesse contexto que a Lei Geral de Proteção de Dados (LGPD) surge como o instrumento regulador de proteção dos direitos fundamentais de liberdade dos cidadãos e cidadãs.

Seja no setor público ou no privado, os pontos trazidos pela lei deverão ser considerados para a estruturação de políticas de confidencialidade, integridade e disponibilidade de dados. Para tanto, faz-se necessário compreender os seus objetivos e de que maneira é possível contribuir para a sua aplicação.

Juan Quirós
Secretário Municipal de Inovação e Tecnologia

ÍNDICE

1. Apresentação
2. Prefácio
3. Glossário LGPD
4. O que é Privacidade e por que devemos protegê-la?
5. O direito à Proteção de Dados Pessoais
6. O Tratamento de Dados Pessoais
   a. Arcabouço normativo da Proteção de Dados
   b. Princípios da Lei Geral de Proteção de Dados
   c. Hipóteses de Tratamento de Dados Pessoais
   d. Compartilhamento de Dados Pessoais
   e. Direitos dos Titulares
   f. Comunicação com a ANPD e com os Titulares de Dados Pessoais
7. Agentes de Tratamento
   a. Definição
   b. Obrigações e Responsabilidades
   c. DPO/Encarregado
8. Segurança da Informação
   a. Incidentes
   b. Relatório de Impacto
   c. Supervisão
   d. Medidas para a mitigação de riscos
   e. Como denunciar um Incidente de Segurança da Informação
9. Como elaborar um Projeto de Adequação à LGPD
   a. Programa de Governança em Proteção de Dados
   b. Estruturação de um comitê de proteção de dados/departamento
   c. Avaliação e Conscientização
   d. Mapeamento de processos
   e. Análise de Gaps
   f. Planejamento
   g. Implementação
   h. Monitoramento
10. Como se proteger no ambiente remoto (reuniões online)
    a. Minimização de exposições pessoais
    b. Segurança da Informação
    c. Vazamento de Dados Pessoais
11. Posfácio

Apresentação

Esta cartilha tem como objetivo fornecer orientações sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.0709/2018. No mundo contemporâneo surgem inovações tecnológicas a todo momento, e diversas inovações tratam Dados Pessoais das mais diversas maneiras. Este tratamento de Dados Pessoais acaba por impactar diretamente a sociedade, influenciando na maneira como as pessoas se relacionam e consomem produtos e serviços.

Por esta razão é essencial a adequação à LGPD, pois a Lei busca uma transformação cultural no que diz respeito ao tratamento de Dados Pessoais e tal transformação que deve alcançar toda a sociedade, empresas, fundações, órgãos e secretarias públicas, bem como o cidadão, que é o titular de seus Dados Pessoais. Essa transformação cultural envolve considerar a privacidade e a proteção de Dados Pessoais em todos os âmbitos e em todas as atividades desenvolvidas na sociedade, desde a concepção de uma atividade até a exclusão dos Dados Pessoais tratados.

O objetivo desta cartilha é contribuir com a implementação e com a compreensão da LGPD, desta maneira, ela foi construida nos seguintes capítulos:

- O capítulo 1 contém um prefácio, com uma frase do grande professor, advogado e PhD, Danilo Doneda;
- O capítulo 2 contempla um glossário, com os principais termos que serão utilizados nesta cartilha;
- O capítulo 3 contém um breve texto sobre privacidade e a razão pela qual devemos protegê-la;
- O capítulo 4 contém um pequeno texto sobre o direito à proteção de Dados Pessoais;
- O capítulo 5 versa sobre o tratamento de Dados Pessoais, as normas, princípios, hipóteses de tratamento e de compartilhamento que o regem, bem como os direitos dos titulares e a comunicação que deverá ser feita entre controladores, ANPD e titulares de Dados Pessoais;
- O capítulo 6 dispõe sobre os agentes de tratamento, suas diferenciações e atuações;
- O capítulo 7 é reservado à Segurança da Informação, tema essencial à proteção de Dados Pessoais;
- O capítulo 8 é mais prático e busca ensinar, de maneira simples, como elaborar um projeto de adequação à LGPD;
- Por fim, o capítulo 9 contém um pequeno guia sobre como se proteger em ambiente remoto, principalmente em reuniões online.

Esta cartilha, elaborada entre os meses de julho e agosto de 2020, deve ser atualizada, aperfeiçoada e ampliada permanentemente. Neste momento a LGPD vigora parcialmente, as suas sanções serão aplicáveis apenas a partir de agosto de 2021 e a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela aplicação e por emitir diretrizes sobre a Lei, ainda não está em funcionamento.

"Privacidade: algo de difícil conceituação, mas sempre condicionada pelo estado da tecnologia em cada época" (DONEDA, Danilo, Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados – 2ª Ed. – São Paulo: Thomson Reuters, 2019)

Glossário LGPD

A Lei Geral de Proteção de Dados apresenta conceitos específicos para as expressões mencionadas em seus artigos. Para a facilitação da leitura desta cartilha serão utilizados os seguintes conceitos:

LGPD: Lei Geral de Proteção de Dados – Lei nº 13.709/2018: A LGPD é uma lei que busca uniformizar o tratamento de Dados Pessoais, em suportes físicos e digitais, realizado por Pessoa Natural ou Jurídica de direito público ou privado, independentemente da localização do Titular dos Dados Pessoais, desde que alguma parte do processo de Tratamento dos Dados Pessoais seja realizada em território brasileiro. O objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da Pessoa Natural. Importante mencionar que a LGPD não se aplica a qualquer tipo de dado ou informação, apenas a Dados Pessoais.

Pessoa Natural: Todos os seres humanos, independentemente de idade, sexo, nacionalidade, etnia, saúde ou quaisquer outras características, possuindo direitos e obrigações.

Pessoa Jurídica: Conjunto de Pessoas Naturais que se reúnem com a mesma finalidade, seja a prestação de serviços ou a comercialização de produtos, contando com respaldo do jurídico. A partir do momento de sua criação, a Pessoa Jurídica adquire personalidade e capacidade própria e seus integrantes passam a tomar decisões em nome da Pessoas Jurídica.

Documento Físico e Documento Digital: Os documentos físicos são aqueles elaborados em suportes físicos, por exemplo, em papel. Já os documentos digitais são informações registradas, codificadas em forma analógica ou em dígitos binários, acessíveis e interpretáveis por meio de um equipamento eletrônico.

Dado Pessoal: São quaisquer informações que identificam ou possam identificar uma Pessoa Natural.

Dados que Identificam uma Pessoa Natural: Como e-mail, endereço, números de RG e CPF.

Dados que Possam Identificar Pessoa Natural: Conjunto de informações que juntas podem identificar uma pessoa, como a soma do primeiro nome, ao endereço, e/ou características físicas da Pessoa Natural.

Dado Pessoal Sensível: São os Dados Pessoais de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma Pessoa Natural. A LGPD trouxe um rol limitado de informações que podem ser enquadradas como sensíveis.

Glossário LGPD

Dado Anonimizado: É o Dado Pessoal que passou por processo de anonimização e, portanto, não pode mais identificar uma Pessoa Natural.

Anonimização: É o processo técnico que visa retirar a possibilidade de o Dado Pessoal identificar uma Pessoa Natural de forma irreversível.

Pseudonimização: É a substituição de informação identificável por identificadores artificiais, cifragem, codificação de mensagens e outros.

Banco de Dados: É uma coleção de dados interrelacionados, representando informações sobre um domínio específico.

Data Center: É um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados e sistemas de ativos de rede.

Titular de Dados Pessoais: A Pessoa Natural a quem pertence o Dado Pessoal.

Agente de Tratamento: Qualquer Pessoa Natural ou Jurídica que realize Tratamento de Dado Pessoal.

Controlador: O Agente de Tratamento que determina como todo e qualquer Tratamento de Dados Pessoais ocorrerá.

Operador: O Agente de Tratamento que segue as determinações do Controlador para o Tratamento de Dados Pessoais.

Encarregado/Data Protection Officer (DPO): É o responsável por atuar na comunicação entre Controlador, os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados. Tem, ainda, o papel de disseminar a cultura da Proteção dos Dados Pessoais dentro de uma organização e avaliar as atividades de Tratamento que a organização realiza.

Tratamento: Toda e qualquer operação realizada com Dados Pessoais, sendo 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.

Consentimento: Uma das hipóteses de Tratamento de Dados Pessoais. Os Dados Pessoais poderão ser tratados após a coleta da manifestação do Consentimento do Titular, que deverá ser livre, informada e inequívoca.

> **Manifestação Livre:** A manifestação do consentimento precisa ser livre, ou seja, deve partir da Pessoal Natural e o Titular não pode ser pressionado a consentir.
>
> **Manifestação Informada:** O Titular deve ter acesso prévio, completo e detalhado sobre o Tratamento de seus Dados Pessoais, incluindo sua natureza, objetivos, métodos, duração, justificativa, finalidades, risco, responsabilidades dos agentes de tratamento e benefícios antes de proferir o Consentimento.

Glossário LGPD

Manifestação Inequívoca: Por fim, a LGPD também obriga que a manifestação do Consentimento deve ser inequívoca, não podendo haver dúvidas sobre a manifestação do Titular, ou seja, não pode haver dúvidas que o Titular consentiu com o Tratamento de seus Dados Pessoais. Este ponto pode ser efetuado por escrito, áudio, vídeo ou de qualquer outra forma, desde que apresente linguagem clara, direta e objetiva e que o Controlador tenha meios de comprovar que o Titular se manifestou de forma inequívoca.

Transferência internacional: Quando os Dados Pessoais são transferidos para empresa terceira ou do mesmo grupo econômico localizada fora do país ou armazenados em servidores de empresas estrangeiras.

Órgão de Pesquisa: Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Compartilhamento: Ocorre quando Dados Pessoais são enviados para terceiros. A possibilidade desta prática deve ser expressamente informada ao Titular de Dados Pessoais no momento de sua coleta, uma vez que há também uma extensão de responsabilidades entre as partes.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): O Controlador deve elaborar uma documentação com a descrição dos processos de Tratamento de Dados Pessoais quando tal Tratamento gerar riscos à liberdade civil e aos direitos fundamentais do Titular.

Legitimate Interest Assessment (LIA): É um teste de proporcionalidade em quatro passos, que deverá ser realizado sempre que a base legal para o Tratamento de Dados Pessoais for o interesse legítimo do Controlador. Este teste deverá avaliar: (a) a legitimidade do interesse, isto é, verificar se a finalidade pela qual se busca o Tratamento é, efetivamente, legítima e, além disso, se a situação é concreta; (b) a necessidade do referido Tratamento, ou seja, se o Tratamento é realizado de forma menos intrusiva possível, em conformidade com o princípio da minimização e, ainda, se existem outras bases legais que podem estruturar tal Tratamento de forma menos onerosa; (c) o balanceamento entre o Tratamento que se pretende realizar e a legítima expectativa do Titular, assim como a não infringência de direitos e liberdades fundamentais; e, por fim (d) estabelecer salvaguardas e garantias que assegurem ao titular a transparência, mecanismos de oposição e a mitigação de riscos.

Glossário LGPD

Autoridade Nacional de Proteção de Dados (ANPD): É a Autoridade criada para oferecer as diretrizes de regulamentação e fiscalização de cumprimento da LGPD, que poderá promover ações educativas, aplicar sanções e multas, além de ser a Autoridade responsável por dirimir dúvidas quanto ao Tratamento de Dados Pessoais em situações concretas.

Bases Legais: Normativos jurídicos que autorizam o tratamento de Dados Pessoais.

Privacy by Design: Também conhecida como Privacidade desde a Concepção, significa levar o risco de privacidade em conta em todo o processo de concepção de um novo produto ou serviço.

Privacy by Default: Também conhecida como Privacidade por Padrão, significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por padrão, apenas seja recolhida/coletada, utilizada e conservada para cada atividade a quantidade necessária de Dados Pessoais.

O que é Privacidade e por que devemos protegê-la?

A privacidade se tornou uma questão passível de proteção pelo Estado somente ao final do século XIX, quando foram inventadas as câmeras de fotografia instantâneas e iniciou a ampla circulação de jornais. Ocorreu, então, a intrusão de um jornalista em uma festa de casamento da sociedade americana, que publicou fotos em um jornal, causando grande aborrecimento aos envolvidos.

Por muito tempo a privacidade foi associada a uma busca de alguma forma de isolamento, refúgio ou segredo, o chamado "direito de estar só". Entretanto, com o passar do tempo e com a evolução tecnológica, o conceito de privacidade foi se relacionando a outras questões, como a busca por igualdade, liberdade de escolha, vontade de não ser discriminado, e até mesmo o desenvolvimento da personalidade.

O Brasil iniciou a proteção à privacidade na Constituição do Império, em 1824. Já estavam presentes em tal Constituição o direito à inviolabilidade do domicílio e a inviolabilidade de correspondências. A atual Constituição Federal de 1988, em seu Art. 5º, incisos X e XII, garante a proteção à intimidade e assegura a inviolabilidade do sigilo de correspondência e das comunicações, protegendo assim diversos aspectos que garantem a privacidade dos cidadãos brasileiros.

A proteção à privacidade é essencial para o ser humano. Todos temos o direito a não sermos incomodados, ou o direito a termos as nossas comunicações livres de interferências, e informações que não devem ser de conhecimento público, ou mesmo o direito a ficar sozinho.

O direito à proteção de Dados Pessoais

Conforme vimos no capítulo anterior, o direito à privacidade está intimamente relacionado aos avanços tecnológicos. Se no final do século XIX, a tecnologia que invadia a privacidade das pessoas eram câmeras fotográficas e jornais que expunham as fotos para todos, hoje em dia, as demandas necessárias para proteger a nossa privacidade são muito diferentes. A tecnologia, em seu estado atual, é capaz de nos conhecer intimamente, entender os nossos hábitos e interesses.

Cada vez mais somos identificados a partir dos nossos Dados Pessoais, fornecidos por nós mesmos a empresas privadas (como planos de saúde e redes sociais) e órgãos públicos (como a declaração de Imposto de Renda). Tais Dados Pessoais podem passar por diversas formas de tratamento, e, ao formar um grande conjunto de Dados Pessoais, podem compor o perfil de uma pessoa e torná-la identificável. Portanto, os Dados Pessoais passam a ser um indicativo de nossa personalidade e merecem proteção.

Algumas formas de tratamento de Dados Pessoais podem implicar em na perda de autonomia em tomadas de decisões, perda da individualidade e até mesmo da liberdade. Nossos Dados Pessoais, estruturados em grandes bancos de dados, são o principal fator considerado em uma avaliação de crédito, na aprovação de um plano de saúde, na obtenção de um emprego, na passagem pelos prgãos de migração em aeroportos e em outras inúmeras situações.

Ademais, o tratamento de Dados Pessoais pode ser uma grande fonte de renda para empresas privadas, que geram grandes bancos de dados com Dados Pessoais, hábitos de consumo, indicativos de personalidade e até mesmo informações íntimas e de caráter privado sobre milhares de pessoas e os vendem para outras empresas, com finalidades diversas, como divulgação de produtos por e-mail e por mensagens de texto.

Desta forma, o tratamento de Dados Pessoais requer instrumentos que o harmonize com os parâmetros de proteção da pessoa natural presentes nos direitos fundamentais e colocados em operação por instrumentos regulatórios que possibilitam aos cidadãos um efetivo controle em relação aos seus Dados Pessoais.

O Tratamento de Dados Pessoais

a. Arcabouço normativo da Proteção de Dados

A temática da Proteção de Dados Pessoais há bastante tempo é discutida e regulamentada fora do Brasil. Na Europa é possível observar uma evolução constante neste debate, desde os anos de 1970. Como já vimos nesta Cartilha, a proteção de Dados Pessoais é uma das facetas do conceito de privacidade e é de grande importância atualmente. Neste ponto veremos quais leis brasileiras antecederam a LGPD e demonstraremos como os assuntos de privacidade e proteção de Dados Pessoais já estavam difundidos na legislação antes do advento da respectiva Lei.

(i) Constituição da República Federativa do Brasil de 1988: a atual Constituição Federal possui a previsão legal de inviolabilidade da intimidade, vida privada, honra e imagem pessoal, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. Também possui a previsão legal da inviolabilidade da correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas.Por fim, prevê o direito ao habeas data, que explicaremos mais adiante.

(ii) Código Civil, Lei 10.406/2002: o Código Civil contém, em seu Capítulo II, disposições sobre os Direitos da Personalidade, que são intransferíveis e irrenunciáveis. Dentre tais direitos estão o direito ao nome e à inviolabilidade da vida privada.

(iii) Código de Defesa do Consumidor, Lei nº 8.078/1990: o Código de Defesa do Consumidor assegura aos consumidores que tenham acesso às informações existentes em cadastros, fichas, registros e Dados Pessoais e de consumo arquivados que versem sobre ele próprio.

(iv) Lei do Habeas Data, Lei nº. 9.507/1997: o habeas data é um instrumento constitucional que busca assegurar aos cidadãos o conhecimento de informações sobre si que constem em registros e bancos de dados de entidades governamentais ou de caráter público.

(v) Lei de Acesso à Informação, Lei nº 12.527/2011: é a primeira legislação a definir o que são Dados Pessoais com a definição que temos hoje na LGPD e a primeira legislação a proteger os Dados Pessoais como uma exceção à transparência intrínseca às democracias. Ainda, tal legislação responsabiliza o Poder Público caso haja dano em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais.

(vi) Lei do Cadastro Positivo, Lei nº 12.414/2011: a Lei do Cadastro Positivo versa, em relação aos Dados Pessoais, como devem ser tratados, sobre a revisão de informações incorretas, e a finalidade para a qual são coletados.

(vii) Marco Civil da Internet, Lei nº 12.965/2014 e Decreto nº 8.771/2016: o Marco Civil da Internet assegura como princípio ao uso da internet a proteção aos Dados Pessoais, e, como direito dos cidadãos, o não fornecimento de seus Dados Pessoais (exceto se houver ordem judicial em específico para tanto). Ainda, instrui como empresas provedoras de conexão à internet e provedoras de conteúdo devem agir quanto à guarda e fornecimento de Dados Pessoais. O Marco Civil da Internet também prevê a figura do consentimento, porém de uma forma diferente do disposto na LGPD (devendo ser livre, expresso e informado). Por sua vez, o seu Decreto regulamentador, possui todo um capítulo que versa sobre a proteção que deve ser empregada aos Dados Pessoais e às comunicações privadas que ocorrem em ambiente virtual, além de ser a primeira legislação nacional a prever o princípio da minimização de Dados Pessoais (previsto na LGPD como o princípio da necessidade, como veremos adiante).

(viii) Lei Geral de Proteção de Dados, Lei nº 13.709/2018: a LGPD assegurar uma uniformidade nas atividades de tratamento de Dados Pessoais no Brasil. Assegura direitos e prevê obrigações aos agentes de tratamento e aos titulares de Dados Pessoais. A vigência da LGPD terá início em 18/09/2020, e as suas sanções serão aplicadas a partir de 01/08/2021.

(ix) Decreto Municipal Regulamentador da LGPD, Decreto 59.767/2020: Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta.

b. Princípios da Lei Geral de Proteção de Dados

A LGPD, possui, além da boa-fé, 10 princípios que devem ser observados por todos que tratem Dados Pessoais. Assim, todas as atividades de tratamento de Dados Pessoais devem observar os seguintes princípios:

(i) Finalidade: simboliza que as finalidades para tratamento de Dados Pessoais devem ser legítimas, específicas, explícitas e informadas ao Titular.

(ii) Adequação: significa que as atividades devem ser compatíveis com as finalidades informadas ao Titular.

(iii) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com a utilização de Dados Pessoais pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.

(iv) Livre Acesso: garantia, aos Titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus Dados Pessoais, bem como sobre a integralidade de seus Dados Pessoais.

(v) Qualidade dos Dados Pessoais: assegura aos Titulares o direito de que os Dados Pessoais estejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

(vi) Transparência: garante aos Titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. A transparência pode ser passiva, atendendo ao Titular sempre que este solicitar informações sobre o tratamento de seus Dados Pessoais, e a transparência pode ser ativa, feita de ofício, de maneira a deixar clara a finalidade do tratamento e seus aspectos legais.

(vii) Segurança: obriga os agentes de tratamento de Dados Pessoais que utilizem medidas técnicas (como o uso de antivírus, firewall e controles de rede) e administrativas (como Políticas de Segurança da Informação e a documentação de processos que ocorrem dentro da organização) aptas a proteger os Dados Pessoais.

(viii) Prevenção: obriga os agentes de tratamento de Dados Pessoais que adotem medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais, ou seja, devem ser adotadas medidas antes que incidentes ocorram.

(ix) Não-Discriminação: impossibilita o tratamento de Dados Pessoais para fins discriminatórios ilícitos ou abusivos, o que já é intrínseco à própria ordem jurídica.

(x) Responsabilização e Prestação de Contas: os agentes de tratamento de Dados Pessoais devem adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, atestar a eficácia dessas medidas.

c. Bases Legais para o Tratamento de Dados Pessoais

Para que uma atividade de Tratamento de Dados Pessoais seja realizada é necessário saber sob qual fundamento de legalidade esta atividade está baseada. A Lei de Acesso à Informação estabelece que, em regra, há necessidade de previsão legal ou consentimento do Titular de Dados Pessoais para que tais atividades ocorram. O princípio constitucional da Legalidade assegura que todas as ações que envolvam o Poder Público devem estar amparadas em disposições legais, incluindo a atribuição de tratar Dados Pessoais.

A LGPD afirma que todo tratamento de Dados Pessoais pelo Poder Público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Assim, sempre deve haver uma norma legal que fundamente, em algum nível, o tratamento de Dados Pessoais. A LGPD estabelece as seguintes bases legais para o tratamento de Dados Pessoais, conforme abaixo:

(i) Consentimento: o consentimento se alinha à ideia da autodeterminação informacional do indivíduo, que significa que a pessoa pode escolher fornecer as suas informações para alguém ou não, exigindo uma participação ativa e, consequentemente, um maior controle sobre o fluxo de suas informações pessoais. O consentimento tem algumas características que lhes são peculiares e para ser considerado válido, deverá ser livre, informado e inequívoco e fornecido para uma determinada finalidade. Esta base legal deve ser utilizada com muita cautela, uma vez que um dos direitos do Titular de Dados Pessoais é exatamente o direito à revogação do consentimento, como veremos mais adiante no tópico sobre os direitos do Titular. Na hipótese de o Poder Público comunicar ou compartilhar Dados Pessoais, será necessário colher o consentimento do Titular, exceto nas hipóteses de dispensa de consentimento, que são tratadas abaixo.

Vigência dada pela Medida Provisória n. º959 de 2020, sendo a redação vigente no momento da confecção desta Cartilha

(ii) Para o cumprimento de uma obrigação legal ou regulatória: quando há a necessidade de tratamento de Dados Pessoais por conta do ordenamento jurídico ou perante o próprio regulador de determinado segmento econômico.

(iii) Pela Administração Pública: para o tratamento e uso compartilhado de Dados Pessoais necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. A LGPD possui um capítulo inteiro sobre o tratamento de Dados Pessoais pela Administração Pública. A grande questão no desenvolvimento de políticas públicas estruturadas em Dados Pessoais é equilibrar a relação entre o Poder Público e os direitos dos cidadãos. O tratamento de Dados Pessoais pelo Poder Público deve se orientar por meio dos princípios gerais de proteção de Dados Pessoais, que vimos acima, e, além disso, buscar equacioná-los com os princípios norteadores da própria Administração Pública. A ratificação de políticas públicas deve sempre buscar diminuir a assimetria que há entre o Estado e os cidadãos.

(iv) Realização de estudos por Órgão de Pesquisa: desde que garantida, se possível, a anonimização ou pseudonimização dos Dados Pessoais. Para compreender perfeitamente esta base legal é necessário observar a conceituação de órgão de pesquisa situada no glossário desta cartilha.

(v) Execução de contratos em que o Titular seja parte: esta base legal poderá ser utilizada quando: (a) o tratamento seja estritamente necessário para a execução de contrato do qual o titular seja parte, ou (b) quando o tratamento for necessário no contexto contratual. Isto ocorre, por exemplo, em atividades de tratamento de Dados Pessoais que decorrem de um contrato de prestação de serviço.

(vi) Exercício regular de direitos em processo judicial, administrativo ou arbitral : trata-se de uma base legal bastante ampla e autoriza o tratamento de Dados Pessoais em processos de qualquer tipo. Portanto, Dados Pessoais que constarem em bases de dados relacionadas aos processos devem sempre respeitar as finalidades pelas quais foram disponibilizadas.

(vii) Proteção da vida ou da incolumidade física do titular ou de terceiros: esta é uma base legal muito importante, pois permite o tratamento de Dados Pessoais quando um titular estiver em risco de vida, como, por exemplo, quando um cidadão é levado a um hospital após sofrer um grave acidente.

(viii) Para a tutela da saúde, em procedimento realizado por profissionais da saúde: é utilizada quando, por exemplo, um cidadão se dirige a uma farmácia para obter remédios.

(ix) Para atender aos interesses legítimos do controlador ou de terceiros: pode ser utilizada para fundamentar atividades de tratamento de Dados Pessoais que tenham finalidades legítimas, consideradas a partir de situações concretas, como apoio e promoção de atividades do Poder Público, e para proteger os Titulares de Dados Pessoais do exercício regular de seus direitos ou prestação de serviços que o beneficiem. Esta é uma base legal complexa, uma vez que, ao tratar Dados Pessoais sob tal hipótese, há a necessidade de elaboração de um relatório de impacto que pode ser exigido pela ANPD, o chamado Legitimate Interest Assessment (LIA). Trata-se de um teste de proporcionalidade em quatro passos e deverá avaliar: (a) a legitimidade do interesse, isto é, verificar se a finalidade pela qual se busca o tratamento é, efetivamente, legítima e, além disso, se a situação é concreta; (b) a necessidade do referido tratamento, ou seja, se o tratamento será realizado de forma menos intrusiva possível, em conformidade com o princípio da minimização e, ainda, se existem outras bases legais que podem estruturar tal tratamento de forma menos onerosa; (c) o balanceamento entre o tratamento que se pretende realizar e a legítima expectativa do Titular, assim como a não infringência de direitos e liberdades fundamentais; e, por fim, (d) estabelecer salvaguardas e garantias que assegurem ao Titular a transparência, mecanismos de oposição e a mitigação de riscos.

(x) Para a proteção do crédito: a proteção do crédito como base legal para o tratamento de Dados Pessoais criou um microssistema de proteção de Dados Pessoais em que, para esses casos, há o convívio pleno e integrado entre diversas normas consumeristas, por exemplo, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e a própria LGPD. Portanto, a referida base legal estrutura efetivamente um sistema em que se busca a proteção do crédito.

É importante informar que, para o caso de Tratamento de Dados Pessoais Sensíveis não poderá ser utilizada a base legal de Interesses Legítimos do Controlador ou de terceiros. Por sua vez, o consentimento, no caso de Dados Pessoais Sensíveis, deverá ser específico e destacado e para finalidades específicas. Ou seja, este consentimento é diferente do consentimento necessário para o tratamento dos Dados Pessoais comuns. Para que sejam tratados Dados Pessoais Sensíveis sob a base legal do consentimento, o Titular precisará ser informado exatamente para quais finalidades os seus Dados Pessoais serão tratados e deverá expressar o seu consentimento em uma cláusula em separado e em destaque do contrato original, como, por exemplo, assinando um anexo.

Ainda, há outra base legal para o tratamento de Dados Pessoais Sensíveis, que é para a garantia de prevenção à fraude e à segurança do Titular, em processos de identificação e autenticação de cadastro em sistemas eletrônicos, ou seja, quando, por exemplo, utiliza-se a biometria para acessar uma conta em um caixa eletrônico.

O Tratamento de Dados Pessoais

Por fim, para o tratamento de Dados Pessoais Sensíveis, sem o fornecimento do consentimento pelo titular, será possível utilizar as outras bases legais explicadas acima, como: (a) o cumprimento de obrigação legal ou regulatória pelo controlador; (b) pela Administração Pública, para a execução de políticas públicas previstas em leis ou regulamentos; (c) a realização de estudos por órgão de pesquisa; (d) o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; (e) a proteção da vida ou da incolumidade física do titular ou de terceiro; e, por fim, (f) a tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

No que tange ao Tratamento de Dados Pessoais de menores de idade, a LGPD informa que este deverá ser realizado em seu melhor interesse. Para tratar Dados Pessoais de crianças (a pessoa até doze anos de idade incompletos) é necessário o consentimento específico e em destaque, dado por pelo menos um dos pais ou responsável legal. Quando houver o tratamento de Dados Pessoais de crianças, os controladores deverão manter informações pública sobre quais são os dados coletados, como ocorre o tratamento e quais os procedimentos para o exercício dos direitos do titular.

Há exceção para o tratamento de Dados Pessoais de crianças. Tais Dados Pessoais poderão ser tratados sem o consentimento de um dos pais ou responsável legal quando a coleta for necessária para contatá-los. Estes Dados Pessoais deverão ser utilizados apenas uma única vez, sem a possibilidade de armazenamento e em nenhum caso poderão ser repassados a terceiros sem o consentimento de um dos pais ou responsável legal.

Ainda, em relação ao tratamento de Dados Pessoais de crianças, os controladores não poderão condicionar a participação em jogos ou em aplicações de internet, ou outras atividades, ao fornecimento de Dados Pessoais, além das informações estritamente necessárias à atividade.

Por fim, o controlador deve envidar esforços para verificar que o consentimento foi dado por um dos pais ou responsável legal pela criança e as informações sobre o tratamento de tais Dados Pessoais deverão ser fornecidas de maneira simples, clara e acessível, para que as próprias crianças possam compreender o que ocorrerá com seus Dados Pessoais. Poderão ser utilizadas cartilhas, vídeos, desenhos animados e quaisquer outros formatos que sejam interessantes às crianças.

Por sua vez, no que se refere ao tratamento de Dados Pessoais de adolescentes (a pessoa entre doze e dezoito anos de idade), a LGPD não faz distinção.

d. Compartilhamento de Dados Pessoais

A LGPD estabelece que os Dados Pessoais tratados pelo Poder Público deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado com seus diversos órgãos e esferas, com vistas à execução de políticas públicas, para a prestação de serviços públicos, para a descentralização da atividade pública e para a disseminação e acesso das informações pelos cidadãos em geral.

O Poder Público só poderá compartilhar Dados Pessoais se tal atividade atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, sempre respeitando aos princípios da Lei, expostos no item "b" desta seção.

O Poder Público poderá compartilhar Dados Pessoais constantes de bases de dados a que tenha acesso nas seguintes situações: (a) em casos de execução descentralizada da atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação; (b) nos casos em que os Dados Pessoais forem acessíveis publicamente; (c) quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres, que deverão ser comunicados à ANPD; ou (d) na hipótese de a transferência dos Dados Pessoais objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do Titular dos Dados Pessoais, desde que vedado o tratamento para outras finalidades.

e. Direitos dos Titulares

Conforme vimos acima, a LGPD unifica uma série de leis que já existiam anteriormente e unifica a forma como os Dados Pessoais devem ser tratados. Diversas legislações já proporcionavam direitos aos Titulares de Dados Pessoais, como o Código de Defesa do Consumidor. Porém, a LGPD inovou ao trazer diversos direitos aos Titulares de Dados Pessoais.

Inicialmente a LGPD informa que toda pessoa natural tem assegurados e garantidos os seus direitos fundamentais de liberdade, intimidade e privacidade, o que é essencial, pois, como vimos no início desta cartilha, a Proteção de Dados é um dos direitos que visam complementar tais direitos. Os demais direitos garantidos ao Titular de Dados Pessoais são:

(i) Confirmação da existência de tratamento;

(ii) Acesso aos dados;

(iii) Correção de dados incompletos, inexatos ou desatualizados;

(iv) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;

(v) Portabilidade dos Dados Pessoais, ou seja, a transferência dos Dados Pessoais de um controlador a outro, desde que assegurados os segredos industrial e comercial;

(vi) Eliminação dos Dados Pessoais tratados sob a base legal do consentimento;
(vii) Informações sobre o compartilhamento de Dados Pessoais;
(viii) Informações sobre a possibilidade de não fornecer o consentimento e sobre as consequências de tal negativa;
(ix) Revogação do consentimento.

f. Comunicação com a ANPD e com os titulares de Dados Pessoais

As pessoas jurídicas de direito público deverão indicar um Encarregado pelo Tratamento de Dados Pessoais, que terá como função se comunicar com a ANPD e com os titulares de Dados Pessoais, prestando informações a respeito das atividades de tratamento de Dados Pessoais realizadas, ou outras, quando solicitadas.

Ainda, a ANPD deverá regulamentar diversos pontos sobre a LGPD e fiscalizará o cumprimento da legislação. Com relação ao Poder Público, a ANPD poderá dispor sobre as formas de que o Poder Público poderá se utilizar para dar publicidade às operações de tratamento de Dados Pessoais.

g. O término do tratamento dos Dados Pessoais

O tratamento de Dados Pessoais não pode ser eterno. Por esta razão a LGPD se preocupou em especificar sob quais hipóteses poderá ocorrer o término do tratamento. Vejamos abaixo:

(i) Quando a finalidade do tratamento for alcançada, ou quando os Dados Pessoais deixarem de ser necessários para o alcance da finalidade almejada;
(ii) O fim do período pelo qual o Dado Pessoal foi coletado;
(iii) A pedido do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público;
(iv) Determinação da ANPD, ou quando houver violação ao disposto na LGPD.

h. A eliminação dos Dados Pessoais

Os Dados Pessoais poderão ser eliminados após o término de seu tratamento, observados os limites técnicos empregados, ou seja, nem sempre será possível eliminar os Dados Pessoais de uma organização, principalmente quando pensamos em Dados Pessoais armazenados em arquivos antigos ou físicos. Poderão ser armazenados os Dados Pessoais para as seguintes finalidades:

(i) Cumprimento de obrigação legal ou regulatória pelo controlador, ou seja, quando um dispositivo legal determinar que o Dado Pessoal seja armazenado por maior período de tempo;
(ii) Estudo por órgão de pesquisa, garantida quando possível a anonimização de tais Dados Pessoais;
(iii) Quando o Dado Pessoal for transferido a terceiro, como, por exemplo, quando um Dado Pessoal for compartilhado com um prestador de serviço, o que tornará impossível ao agente de tratamento original solicitar a exclusão de tal Dado;
(iv) Quando o controlador fizer uso exclusivo de tais Dados Pessoais, desde que estes sejam anonimizados.

Agentes de Tratamento

Encarregado pelo Tratamento de Dados Pessoais
Profissional responsável por acompanhar todas as atividades que dizem respeito à Proteção de Dados Pessoais, disseminação da cultura e dos valores referentes à LGPD, bem como ser o ponto focal para a comunicação interna da organização, para a comunicação com os titulares de Dados Pessoais e com a ANPD.

Controlador de Dados Pessoais
A Pessoa Física ou Jurídica que determina como todo e qualquer Tratamento de Dados Pessoais ocorrerá.

Operador de Dados Pessoais
A Pessoa Física ou Jurídica que segue as determinações vindas do Controlador para elaborar o Tratamento de Dados Pessoais.

a. Definição
A LGPD define a figura dos agentes de tratamento de Dados Pessoais como os indivíduos que controlam ou tratam informações que contenham Dados Pessoais. A lei elenca expressamente, no artigo 5º, inciso IX, que os agentes de tratamento são definidos como Controlador e o Operador.

A diferença entre o Controlador e o Operador está no escopo da função: o Controlador coleta os Dados Pessoais dos Titulares de dados e a ele compete as decisões quanto ao Tratamento dos Dados Pessoais obtidos.

O Operador tratará os Dados Pessoais em nome do Controlador, isto é, realizará o Tratamento de Dados Pessoais em virtude de contrato, respeitando as instruções do Controlador.

b. Obrigações e Responsabilidades
A LGPD diferencia os agentes de tratamento e dispõe sobre as obrigações e responsabilidades no caso de ressarcimento de danos decorrentes do tratamento inadequado de Dados Pessoais e no caso de incidentes de segurança da informação.

A principal obrigação que a lei dispõe aos agentes acima citados, é a de que mantenham um registro das operações de tratamento que realizarem, especialmente quando este Tratamento de Dados Pessoais for realizado segundo a base legal do legítimo interesse.

Por sua vez, é dever do Operador realizar o Tratamento de Dados Pessoais conforme as instruções fornecidas pelo Controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. É necessário que todas as instruções a serem cumpridas sejam claras e, preferencialmente, formais, para que não haja incerteza ou falha no processo de Tratamento de Dados Pessoais.

O agente de tratamento que, em razão do tratamento inadequado 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. Nesse sentido, o Operador, apesar de tratar os dados conforme as instruções fornecidas pelo Controlador, também poderá ser responsabilizado a reparar o dano causado.

c. Encarregado pelo Tratamento de Dados Pessoais /Data Protection Officer (DPO)

A LGPD, em seu artigo 5º, inciso VIII, designa a criação do cargo de Encarregado de Proteção de Dados Pessoais, figura também conhecida como Data Protection Officer (DPO). Este profissional será o responsável na empresa por acompanhar todas as atividades que dizem respeito à proteção de Dados Pessoais, bem como ser o ponto focal para a comunicação interna da Empresa, para a comunicação com os titulares de Dados Pessoais e com a ANPD.

A imputação da necessidade de um Encarregado busca garantir que as informações sobre proteção de Dados Pessoais sejam centralizadas dentro da organização. O cargo poderá ser ocupado por uma pessoa física ou jurídica, que poderá ser interna ou externa, ou até mesmo em um modelo híbrido, com contratados internos e externos ao mesmo tempo. Ainda, poderá ser um departamento, com pessoas de diversas áreas, a fim de que possam cumprir com as diversas funções que o Encarregado possui.

Ainda, o Encarregado tem a atribuição de fazer a gestão das reclamações e comunicações dos titulares de Dados Pessoais, receber comunicações da ANPD, orientar os funcionários e contratados da empresa sobre boas práticas a serem adotadas em relação à proteção de dados, o que compreende elaborar treinamentos, revisar políticas e procedimentos internos, conscientizar os funcionários sobre a importância da LGPD e mitigar riscos de incidentes de segurança da informação, e, por fim, executar as demais atribuições que a empresa lhe atribuir.

O profissional deverá ter autonomia para auditar e fiscalizar as possíveis irregularidades, a fim de serem corrigidas e notificadas conforme rege a lei, não podendo, portanto, haver conflito de interesses entre suas funções, caso as acumule.

d. Comitê de Privacidade e Proteção de Dados Pessoais

O Comitê de Privacidade e Proteção de Dados Pessoais deve atuar em conjunto com o DPO para auxiliar no desenvolvimento de algumas atividades ligadas à organização, como:

Agentes de Tratamento

- Facilitar a promoção de uma cultura de Proteção aos Dados Pessoais dentro da organização;
- Propor Políticas de Segurança da Informação;
- Gerenciar atividades relacionadas ao Tratamento de Dados Pessoais, bem como avaliar se estão de acordo com as normas de Proteção aos Dados Pessoais;
- Fiscalizar processos que envolvam o Tratamento de Dados Pessoais;
- Realizar treinamentos para os funcionários da organização, fornecedores e terceiros sobre a importância da Proteção aos Dados Pessoais.

A PRODAM-SP conta com um Comitê de Privacidade e Proteção de Dados Pessoais, composto por cinco membros, sendo cada um proveniente de cada uma das áreas inter nas listadas abaixo:

- Gerência de Conformidade, Gestão de Riscos e Controle Interno;
- Ouvidoria;
- Diretoria Jurídica;
- Gestão de Pessoas;
- Diretoria de Infraestrutura e Tecnologia.

Segurança da Informação

Segurança da Informação é um conjunto de mecanismos e ferramentas que uma empresa utiliza com a finalidade de proteger um conjunto de informações, para preservar o valor que tais informações geradas pela empresa possuem. É, assim, um conjunto de regras essencial a empresas, principalmente para aquelas que lidam com informações valiosas e sigilosas.

Sob a LGPD, os Controladores e Operadores devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os Dados Pessoais de acesso não autorizado, destruição, perda, modificação, comunicação ou outros tipos de tratamento não autorizados ou ilegais. Espera-se que a ANPD forneça, no futuro, diretrizes para padrões técnicos mínimos.

O Marco Civil da Internet e seu Decreto Regulamentador estabelecem as seguintes diretrizes sobre normas de segurança que devem ser observadas pelos provedores de conexão e de aplicação no Tratamento de Dados Pessoais e de comunicações privadas que trafegam pela internet: (a) o estabelecimento de controles rígidos sobre o acesso a Dados Pessoais, estabelecendo responsabilidades para aqueles que terão acesso a Dados Pessoais; (b) o fornecimento de mecanismos de autenticação para o acesso a registros, usando, por exemplo, sistemas de autenticação dupla para garantir a individualização dos responsáveis pelo Tratamento de Dados Pessoais; (c) a criação de inventários detalhados de logs referentes à conexão e ao acesso aos aplicativos, que contenham data, hora, minuto e segundo e a duração do acesso, a identidade do indivíduo que acessou os arquivos e quais arquivos foram acessados; e (d) o uso de soluções de gerenciamento de registros por meio de técnicas que garantam a inviolabilidade dos Dados Pessoais, como criptografia ou medidas de proteção equivalentes.

Além disso, cada setor possui regras específicas quanto a padrões mínimos ou esperados que garantam a segurança da informação das organizações.

Alguns princípios que podem nortear uma Política de Segurança da Informação são: (a) confidencialidade, para que as informações sejam acessadas apenas por pessoas autorizadas; (b) integridade, para que as informações apenas sejam alteradas por pessoas autorizadas; e (c) disponibilidade, ou seja, as informações devem sempre estar disponíveis para quem é autorizado, evitando interrupções no fluxo de trabalho.

a. Incidentes

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil ("CERT.br"), um Incidente de Segurança da Informação pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. Assim, Incidentes de Segurança da Informação é toda e qualquer situação na qual uma entidade que lida com informação está sob risco.

Como exemplos de Incidentes de Segurança da Informação podemos mencionar o acesso de terceiro não autorizado em redes de computadores, ou seja, quando algum agente externo, ou mesmo um funcionário ou colaborador da organização acessa (ou tenta acessar) uma parte do sistema que não deveria.

Os vírus e códigos maliciosos também são caracterizados como Incidentes de Segurança da Informação, e sua detecção requer o uso de ferramentas próprias, como antivírus. Por fim, como último exemplo, podemos citar o uso impróprio de sistemas ou de informações, que ocorrem quando um funcionário da organização usa um e-mail corporativo para a promoção de negócios pessoais, ou quando instala uma ferramenta não autorizada no computador da organização, utiliza um pen drive de forma não autorizada, ou ainda, exemplificando com documentos físicos, imprime documentos sigilosos de forma não autorizada e os repassa para terceiros.

b. Relatório de Impacto à Proteção de Dados Pessoais

A ANPD pode ainda exigir que o Controlador prepare um Relatório de Impacto à Proteção de Dados Pessoais ("RIPD", ou, Data Protection Impact Assessment, "DPIA"), inclusive nos casos em que o Controlador trata Dados Pessoais Sensíveis ou se baseia em Legítimo Interesse como base legal para efetuar o Tratamento. Tal relatório deve conter, pelo menos, uma descrição dos tipos de Dados Pessoais coletados, a metodologia usada para a coleta e a garantia da segurança das informações, e uma análise do Controlador em relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados.
A ANPD regulamentará as disposições que serão necessárias ao RIPD e em quais circunstâncias poderá ser requerido.

Neste momento, a LGPD apenas (i) lista como conteúdo mínimo do RIPD: (a) descrição dos tipos de Dados Pessoais coletados; (b) a metodologia utilizada para a coleta e a garantia de segurança das informações; e (c) uma análise do Controlador em relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados; e (ii) lista duas circunstâncias sob as quais a ANPD pode solicitar o referido relatório, quais sejam: (a) sempre que a base legal para o Tratamento de Dados Pessoais for o interesse Legítimo do Controlador; e (b) sempre que houver o Tratamento de Dados Pessoais Sensíveis.

c. Supervisão

O Supervisor de Tecnologia da Informação é o profissional responsável por supervisionar as atividades de suporte de rede, da área de informática de uma organização, envolvendo a elaboração de projetos de implantação, desenvolvimento e integração de sistemas. São responsabilidades de um Supervisor de Tecnologia da Informação: realizar planejamento de projetos, atender as necessidades e negócios da organização, atuar na parte de dados informáticos da empresa, administrar e controlar o centro de processamento da empresa, fazer instalações e manutenções dos equipamentos informáticos, fazer cumprir as Políticas de Segurança da Informação, dentre muitas outras funções.

d. Medidas para a mitigação de riscos

Dentre as principais medidas que podemos apresentar para a mitigação de riscos envolvendo Incidentes de Segurança da Informação encontram-se desde pontos muito simples, que podem ser adotados no dia a dia das pessoas, como a instalação de um antivírus e a recomendação de não abertura de e-mails de endereços desconhecidos, até mesmo questões mais complexas, como a atualização de sistemas (principalmente os sistemas de proteção e operacionais).

Ainda, importante mencionar a recomendação de estabelecer Políticas de Segurança da Informação e treinamentos a serem ministrados a todos os funcionários de uma organização. É essencial que os funcionários sejam treinados para que saibam como agir diante de situações que podem configurar como uma tentativa de provocar um Incidente e mesmo diante de um Incidente de Segurança da Informação propriamente dito.

Por fim, as Políticas são excelentes maneiras de formalizar como a organização trata os sistemas, informações e processos, e são essenciais para o dia a dia de uma organização.

e. Como denunciar um Incidente de Segurança da Informação?

Ao detectar um Incidente de Segurança da Informação, é essencial que tal ato seja denunciado aos responsáveis dentro da empresa. A denúncia deve poder ser realizada de forma anônima e conter as seguintes informações:

- Data e hora do Incidente;
- Nome da pessoa responsável pelo Incidente, se possível;
- Local onde o Incidente ocorreu/foi realizado;
- Descrição do Incidente;
- Efeitos do Incidente, se for possível detectar tal ponto durante o ato da denúncia;
- Em qual sistema/suporte o Incidente ocorreu (impressora, servidor, e-mail);
- Testemunhas.

Ainda, a organização deve avaliar a necessidade de informar os seus fornecedores, clientes e até mesmo fazer uma nota de esclarecimento na mídia a respeito do Incidente de Segurança da Informação, suas consequências e as medidas realizadas para a mitigação de riscos. No futuro, será necessário também informar tais pontos à ANPD.

Como elaborar um Projeto de Adequação à LGPD

Etapa 1 - Programa de Governança em Proteção de Dados Pessoais
Elaboração de um Programa de Governança em Proteção de Dados Pessoais e disseminação da cultura e dos valores sobre o Tratamento Adequado de Dados Pessoais.

Etapa 2 - Estrutura de Comitê de Proteção de Dados
Estruturação de um Comitê responsável pela adequação da empresa à LGPD.
Neste Comitê devem estar presentes pessoas da alta diretoria e pessoas das áreas que tratem Dados Pessoais.

Etapa 3 - Avaliação e Conscientização
Conscientizar funcionários em relação ao projeto e seu objetivo. Podem ser utilizadas palestras, workshops, apresentações, videoconferências etc.

Etapa 4 - Mapeamento de Processos
Elaboração de Mapeamento de Processos que tratam Dados Pessoais. O Mapeamento deve demonstrar o caminho percorrido pelo Dado Pessoal dentro da organização, desde a sua coleta até o seu descarte. Deve-se analisar a Finalidade para a qual o Dado Pessoal é tratado, se está sob uma Base Legal e se há compartilhamento com terceiros.

Como elaborar um Projeto de Adequação à LGPD

Etapa 5 - Análise de Gaps
Com o Mapeamento de Processos será possível identificar questões em desacordo com a LGPD ou com as melhores práticas de segurança da informação. Deve-se elaborar um Relatório de Adequação que aponte os principais gaps e as medidas necessárias para a mitigação de riscos.

Etapa 6 - Planejamento
Após a análise de gaps será necessário verificar quais as prioridades da organização e elaborar um cronograma para mitigar os riscos localizados.

Etapa 7 - Implementação
Implementar as medidas localizadas no cronograma. Adequação de plataformas, processos, contratos, práticas e documentos que versem sobre o Tratamento de Dados Pessoais.

Etapa 8 - Monitoramento
Análise de novos projetos, novos produtos e novos processos. Constantemente a organização deve avaliar se está de acordo com a legislação referente à Proteção de Dados Pessoais.

Como elaborar um Projeto de Adequação à LGPD

Antes de entrarmos neste capítulo, é importante esclarecer que elaborar um projeto de adequação à LGPD é como fazer uma grande arrumação em um guarda-roupas, porém em manutenção. Antes de começarmos a arrumar um guarda-roupas, precisamos saber quem fará a organização, como será essa organização, se doaremos as roupas ou não, como organizaremos as roupas dentro do armário e por fim, o mais importante, manter as roupas arrumadas para sempre.

Desta forma, segue abaixo um passo a passo de como elaborar um projeto de adequação à LGPD:

a. Programa de Governança em Proteção de Dados

Para garantir o efetivo cumprimento das normas, a LGPD em seu artigo 50, nos traz um capítulo exigindo que sejam formuladas regras sobre boas práticas e governança, que estabeleçam as condições, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de Titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no Tratamento dos Dados Pessoais, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao Tratamento de Dados Pessoais. Além disso, é importante que a cultura e os valores sobre o Tratamento adequado de Dados Pessoais sejam difundidos em toda a sociedade.

Cada política, norma e ação criada dentro da empresa deve ser documentada para demonstrar a efetividade de seu programa de governança, quando houver questionamento e, em especial, a pedido da ANPD. A adoção de políticas de boas práticas e governança não apenas auxilia a empresa a cumprir com as obrigações estabelecidas pela LGPD, como demonstra os esforços nesse sentido e todos os registros documentados das ações adotadas serão considerados em uma eventual aplicação de sanção por Tratamento inadequado de Dados Pessoais.

b. Estruturação de um grupo de trabalho de Proteção de Dados

Para a correta adequação à LGPD pela administração pública, sugerimos a estruturação de um grupo de trabalho que seja responsável pelo Projeto e pelo estudo do tema. É essencial que neste grupo estejam presentes e engajadas pessoas da alta diretoria da Administração, bem como pessoas de áreas que tratam Dados Pessoais em seu dia a dia.

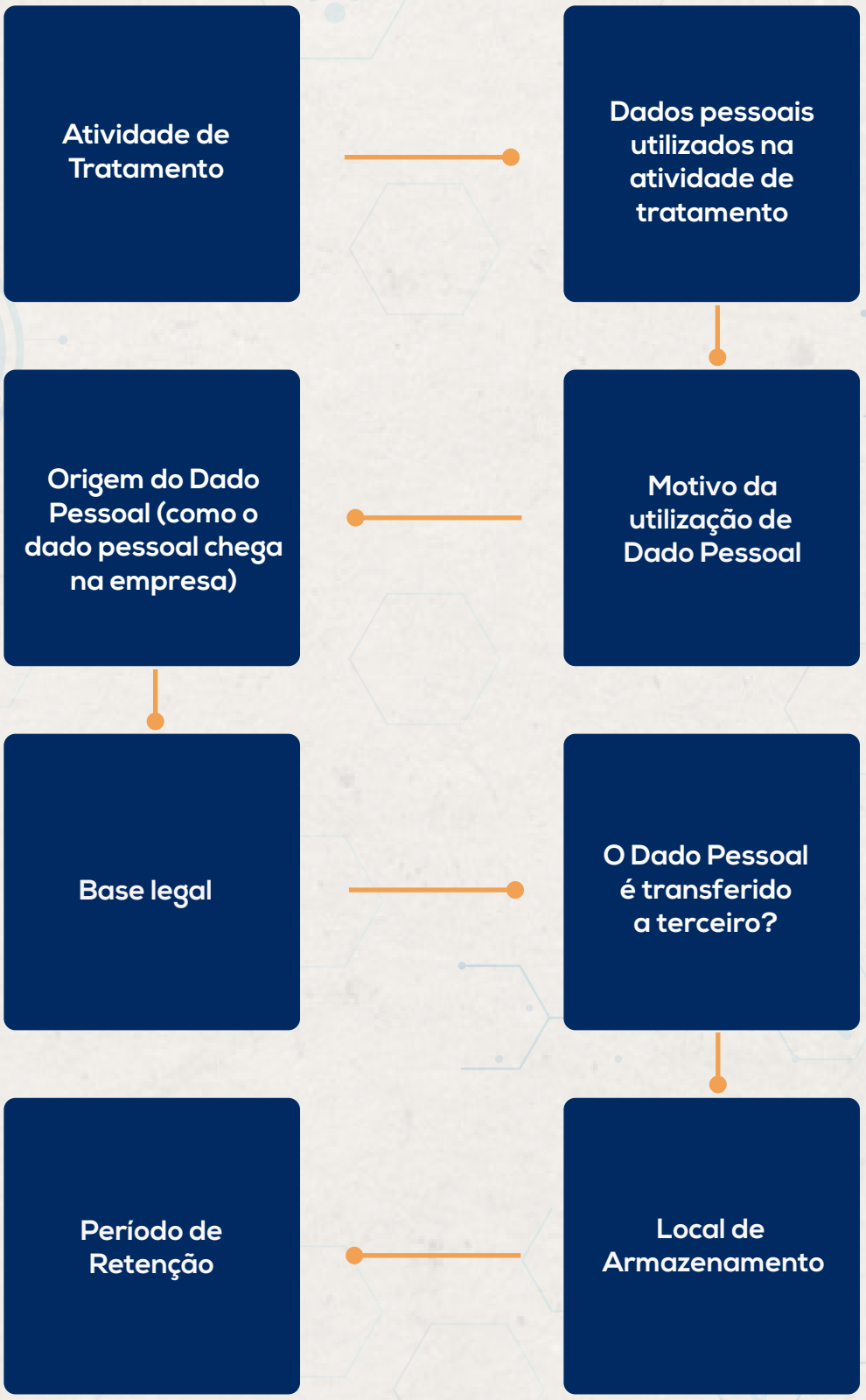
c. Avaliação e Conscientização

O primeiro passo em concreto para a adequação à LGPD deve levar em consideração o quanto de informação sobre o projeto os funcionários possuem. Portanto, é essencial conscientizar os funcionários em relação ao que é projeto e qual o seu objetivo. A conscientização pode ser feita por meio de palestras, apresentações, videoconferências e até mesmo com pequenos informes enviados aos funcionários, periodicamente. A empresa deve se familiarizar com a LGPD, com a metodologia do projeto e entender que todas as atividades serão averiguadas.

Como elaborar um Projeto de Adequação à LGPD

d. Mapeamento de Processos

Em um projeto de adequação à LGPD, o mapeamento de dados é dividido da seguinte forma:



Como elaborar um Projeto de Adequação à LGPD

A LGPD determina que o Controlador e o Operador mantenham registro das operações de Tratamento de Dados Pessoais que realizarem, e o momento em que isso ocorre é durante a etapa de Mapeamento de Processos, que é um passo muito importante para a adequação da empresa.

Neste momento será possível detalhar cada dado pessoal tratado, entendendo as fases do seu ciclo de vida. Será possível entender como os dados são recebidos, como e onde estão armazenados, quem tem acesso, se os dados são compartilhados com terceiros, quais os riscos associados a cada operação e a base legal adequada. Desta forma, será possível analisar a forma como a empresa lida com os Dados Pessoais de seus colaboradores, clientes e parceiros.

e. Análise de Gaps

Após o Mapeamento dos Processos será possível identificar diversas questões em desacordo com a LGPD ou com as melhores práticas de segurança da informação, ou, ainda, com as práticas setoriais aplicáveis. Neste momento deve-se definir as bases legais adequadas para cada atividade de Tratamento de Dados Pessoais executadas na companhia, bem como elaborar um relatório com os principais gaps, apontando quais as medidas necessárias para a mitigação de riscos envolvendo incidentes de segurança da informação.

f. Planejamento

Após analisados os gaps encontrados, será necessário verificar quais as prioridades da empresa e elaborar um cronograma para mitigar os riscos localizados nas etapas anteriores. Será necessária a indicação de responsáveis para cada atividade de Tratamento, com necessidade de alteração e a verificação dos diferentes níveis de criticidade de cada medida.

g. Implementação

É chegada a hora de implementar as medidas encontradas em desconformidade com a legislação. Neste momento será necessário adequar plataformas, processos, contratos, práticas e documentos que versem sobre o Tratamento de Dados Pessoais.

h. Monitoramento

Após a etapa da implementação, chegamos ao final do nosso projeto de adequação à LGPD, porém, é possível dizer que tais projetos chegam a um fim? Acreditamos que, assim como a organização de um guarda-roupa, é necessário sempre manter a ordem. As organizações, em um geral, são organismos vivos, estão em constante mudança, com novos projetos, novos produtos e processos, e desta forma, a etapa de monitoramento não tem fim, pois constantemente a organização deve avaliar se está de acordo com a legislação de proteção de Dados Pessoais.

Como elaborar um Projeto de Adequação à LGPD

Ainda, a própria legislação está em constante alteração e regulamentação, o que mostra que a empresa precisará se adequar às novidades que surgirem no cenário da privacidade.

Desta maneira, é essencial que a organização tenha funcionários (internos, externos, ou mesmo uma equipe híbrida) que sejam capazes de monitorar todas as novidades que podem ocorrer, para nunca deixar a organização desatualizada e sob o risco de sofrer uma sanção pela ANPD.

Outro ponto fundamental do monitoramento é a necessidade de treinamentos em certa periodicidade, para que a cultura da proteção aos Dados Pessoais seja parte do dia a dia da organização.

Como se proteger no ambiente remoto (reuniões online)

A prática de reuniões online se tornou indispensável para o funcionamento de escritórios, escolas, órgãos públicos, organizações e até mesmo reuniões de amigos. É preciso um pouco de cuidado ao realizar reuniões online, uma vez que podem ocorrer vazamentos de informações sigilosas, exposições indevidas e incidentes de segurança da informação.

É essencial que os funcionários da organização sejam treinados para a realização de videoconferências, de maneira a minimizar os eventuais danos que possam ser causados e, inclusive, orientar a respeito do funcionamento da plataforma, regras de conduta, e demais instruções que sejam necessárias.

Por isso, seguem abaixo algumas dicas para se proteger:

a. MINIMIZAÇÃO DE EXPOSIÇÕES PESSOAIS:

a.1 A escolha do ambiente ideal

É importante estar atento ao ambiente físico dentro de sua casa em que você participará da reunião. Escolha um local que não tenha grande circulação e, se possível, feche a porta. É comum que vídeos viralizem pela internet com participações inusitadas em videoconferências, como animais de estimação e crianças.

a.2 Comporte-se

A reunião pode estar acontecendo por videoconferência e você pode estar dentro da sua casa, entretanto é importante que a etiqueta e o comportamento sejam mantidos exatamente como se você estivesse no escritório. Assim, vista-se de acordo com o esperado, arrume os cabelos, lave o rosto, tenha um bloco de anotações à mão e, se possível, indique que gostaria de participar, sem interromper os outros participantes. A pontualidade também é um fator fundamental para o sucesso da reunião.

a.3 O uso de câmeras e microfones

Caso não haja necessidade, deixe sua câmera e seu microfone desligados. Desta forma, haverá menos interrupções durante a reunião. Utilize fones de ouvido com microfone, estes equipamentos são melhores do que o uso do microfone interno do notebook, que pode causar ecos ou distorções. Ainda, prefira áudio ao vídeo, pois se a qualidade de uma conexão for baixa a experiência da reunião poderá ser comprometida.

Como se proteger no ambiente remoto (reuniões online)

b. VAZAMENTO DE DADOS PESSOAIS

b.1 Utilize ferramentas confiáveis e, se possível, criptografadas

Há diversas ferramentas que possibilitam uma reunião online. Pesquise todas as ferramentas disponíveis e veja a que melhor se adeque às necessidades de sua reunião e de sua organização. Opte para que toda a organização utilize a mesma ferramenta, para que o uso seja uniforme e todos saibam utilizá-la adequadamente. Prefira ferramentas que tenham recursos como sala de bate-papo, essencial para a anotação de dúvidas e observações sobre a matéria, e se há modos de indicar quando um participante quiser participar, como a ferramenta de "levantar a mão".

b.2 Políticas e normas de segurança da informação

O vazamento de informações é algo que vem preocupando cada dia mais as organizações e durante o home office as organizações têm dificuldade de monitorar se os seus funcionários estão seguindo todas as diretrizes relacionadas à segurança da informação. Assim, é importante que a organização mantenha treinamentos frequentes relacionados à segurança da informação para os seus funcionários, explique detalhadamente cada norma e cada política, bem como a importância de evitar incidentes.

b.3 Proiba que funcionários gravem as reuniões

Seguindo a linha da segurança da informação, é essencial que os funcionários sejam avisados se é permitida ou não a gravação das reuniões. Durante as videoconferências podem ser expostas informações valiosas sobre a organização, sobre funcionários e mais ativos de informação essenciais para a vida da organização. Desta maneira, é essencial que a organização explique aos funcionários sobre as complicações que podem ser geradas por conta de uma informação disponibilizada a terceiros de maneira ilegal. Ainda, se possível, utilize aplicativos que não permitam gravações de tela, nem o famoso print screen.

b.4 Desative a VPN

Talvez a organização em que você trabalha tenha lhe fornecido um serviço de VPN (Virtual Private Network), que permite que você use a rede da empresa enquanto trabalha remotamente. Muitas vezes a VPN limita a largura de banda larga disponível. Neste caso, você pode fazer as reuniões por videoconferência fora da VPN para ter uma experiência de melhor qualidade.

b.5 Cada usuário deve utilizar um login

Forneça um e-mail e uma senha para cada usuário acessar a reunião. Normalmente são utilizados o e-mail profissional e a senha deste e-mail para a participação em videoconferências, porém, é sempre importante frisar que cada funcionário deve utilizar o seu próprio login e que logins não devem ser compartilhados entre colegas. Esta é uma medida fundamental, que garante que somente acessarão a reunião e as informações disponibilizadas os funcionários autorizados.

Como se proteger no ambiente remoto (reuniões online)

b.6 Faça um disclaimer no convite para a videoconferência

Envie um pequeno manual de como as pessoas devem se comportar durante a videoconferência, quais as principais regras, quais dados pessoais poderão ser tratados e por que serão tratados durante a videoconferência, bem como o respectivo assunto.

c. VAZAMENTO DE DADOS PESSOAIS:

c.1. Fique atento às permissões concedidas aos aplicativos

É essencial que a organização escolha um aplicativo confiável para as videoconferências, conforme destacado acima. Entretanto, os funcionários devem prestar muita atenção às permissões que concedem aos aplicativos, principalmente quando baixados no celular. Suspeite de permissões invasivas e confira os dados aos quais o aplicativo requer acesso para funcionar, que devem ser relacionados apenas ao funcionamento da câmera e do microfone do aparelho celular.

c.2. Desative notificações em pop-up ao compartilhar a tela

Ao compartilhar a tela do computador ou do celular durante chamadas de vídeo é importante desativar notificações em pop-up de e-mails, redes sociais e aplicativos de mensagem. As mensagens podem tratar de assuntos privados desnecessários à reunião.

c.3. Envie o convite da chamada apenas para e-mails confiáveis

Não compartilhe links de convites de chamadas de vídeo pelas redes sociais. Prefira encaminhá-los de forma privada, utilizando o endereço de e-mail dos participantes da reunião. Compartilhar a URL dos convites pode atrair desconhecidos e cibercriminosos para a chamada de vídeo, comprometendo informações dos participantes.

c.4. Evite o phishing

Phishing é um tipo de crime virtual. Trata-se da prática de coletar informações e dados secretos dos usuários através de informações falsas ou dados não reais, porém muito atrativos. Atualmente muitos cibercriminosos utilizam sites semelhantes aos sites dos aplicativos de conferência para "roubar" as informações de logins e senhas de e-mails de pessoas e fazer mau uso de tais informações. Portanto, é importante estar atento aos sites e aplicativos aos quais você fornece suas informações de acesso.

c.5. Atualize o antivírus

O antivírus é um programa de segurança básico e essencial para se ter em qualquer computador. Além de proteger a máquina e os sistemas contra vírus e malwares, ele ainda pode evitar travamentos e a lentidão do computador.

Posfácio

A Cartilha LGPD, desenvolvida pela Prodam em parceira com a P&B Compliance, foi publicada levando em consideração o atual cenário legal sobre o assunto, pautando-se na Lei n.º 13.709/2018 e em suas alterações, trazidas pela Lei n.º 13.853/2019. Outras alterações e complementações poderão ocorrer durante os próximos meses ou anos.

Além disso, são trazidas algumas das boas práticas em segurança da informação e gestão de governança em proteção de dados, assim como "dicas" e informações que serão utilizadas no dia a dia de todo o profissional que faça uso de dados pessoais. O objetivo da cartilha não é esgotar um assunto tão complexo e minucioso, tampouco trazer uma abordagem genérica. Nosso propósito é que ela seja um passo a passo para a adequação à LGPD, uma vez que há diversas particularidades para cada órgão, empresa ou pessoa que trate de Dados Pessoais, desde os tipos de dados, as bases legais que justifiquem seu tratamento, passando pelo volume desses dados e dos ricos de cada um.

Esse trabalho deve ser considerado como um guia inicial, uma referência rápida e a abertura de um trabalho de conscientização para cada funcionário, empregado, colaborador, profissional ou interessado no assunto, mas, principalmente, traga o entendimento que a Proteção dos Dados afeta e atinge a todos nós e passa a ser uma obrigação do profissional moderno, das empresas, governos e governantes do mundo atual.