ahreas

CARTILHA

LGPD

LGPD para empresários individuais, micro e pequenas empresas

1) Breve introdução

A Lei nº 13.709 de 14 de agosto de 2018, conhecida por Lei Geral de Proteção de Dados, a "LGPD", ganhou força com o regulamento europeu, denominado GDPR (General Data Protection Regulation). No Brasil, a LGPD entrou em vigor em 18 de setembro de 2020.

A LGPD possui o objetivo de regrar a coleta, o uso e o armazenamento de dados de pessoas físicas, online ou offline, com o fim de proteger direitos fundamentais, como liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2) Conceitos da LGPD – Como identificar se a sua empresa deve se adequar?

→ A quem se aplica a nova lei? Profissionais liberais, empresários individuais, micro e pequenas empresas, por exemplo, devem se adequar às suas regras? Ou será que vale somente para empresas grandes, multinacionais?

A LGPD traz algumas definições que auxiliam a entender a quem se dirige. Identificando quem são os personagens e o que cada um faz com os dados de pessoas físicas (os dados que são o alvo da proteção da lei) fica mais fácil saber se a sua empresa deve tomar alguma providência para não correr riscos de sofrer penalidades:

- 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, ou seja, o responsável pela coleta e pela forma de tratamento dos dados;

- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

- Dado pessoal: qualquer informação relativa à pessoa natural, o titular, como, por exemplo, o nome, o RG, o CPF, o e-mail, o endereço, o número da conta bancária, etc.;

- Dado pessoal sensível: são os dados pessoais sobre a 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;

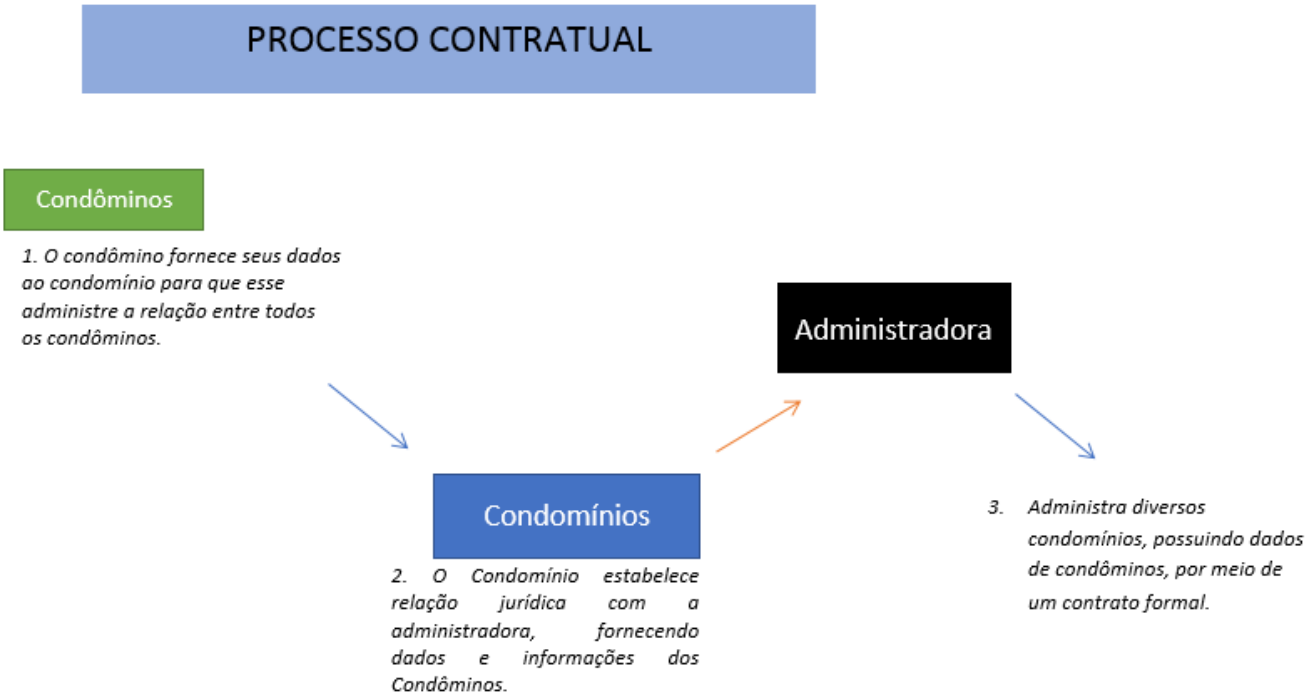
- Tratamento: toda operação realizada com os dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação,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

→ Em resumo, a quem se aplica a LGPD?

Profissional liberal, Empresário individual, Empresa de pequeno porte, Microempresa, Empresas médias e Empresas grandes, que se encaixam nos conceitos de "controlador" e/ou "operador" de dados pessoais e praticam quaisquer das hipóteses que podem ser consideradas como "tratamento", deverão se adequar à nova lei.

3) Aplicação da LGPD nas relações entre administradora de condomínios, condomínios e condôminos

As relações entre Administradoras de Condomínios, Condomínios e Condôminos podem ser assim desenhadas:



Veja como ficam classificados os personagens acima, diante dos conceitos da LGPD:

PERSONAGEM/AÇÃO		CONCEITO DA LEI
CONDÔMINOS	→	TITULAR
CONDOMÍNIOS	→	CONTROLADOR E OPERADOR
ADMINISTRADORA DE CONDOMÍNIOS	→	CONTROLADOR E OPERADOR
COLETA DE DADOS DOS CONDÔMINOS	→	TRATAMENTO
ENVIO DE DADOS DOS CONDÔMINOS PARA EMISSÃO DE BOLETOS	→	TRATAMENTO
ENVIO DE DADOS PELOS CONDOMÍNIOS A ADMINISTRADORA DE CONDOMÍNIOS	→	TRATAMENTO
ENVIO DE DADOS PELA ADMINISTRADORA PARA TERCEIROS PRESTADORES DE SERVIÇOS	→	TRATAMENTO

Com base nesses esclarecimentos fica mais fácil identificar que todas as empresas devem se adequar à LGPD.

→ Identifiquei que minha empresa trata dados pessoais de meus clientes. O que faço agora? Não posso mais usar esses dados?

Pode! Mas alguns cuidados devem ser adotados, veja o próximo tópico.

4) O que as empresas devem fazer para se adequar à nova lei?

O roteiro abaixo auxiliará empresários individuais, micro e pequenas empresas a adotarem algumas medidas para que possam estar em conformidade com a lei. No caso de empresas maiores, ou mesmo se houver alguma dificuldade por parte daquelas, a recomendação é que busquem a assessoria jurídica especializada.

A. DIAGNÓSTICO	B. PROVIDÊNCIAS	C. IMPLANTAÇÃO
1. Faça um levantamento dos procedimentos internos de sua empresa, como nos esquemas das figuras acima, listando o "caminho" dos dados pessoais de clientes (condôminos) desde a chegada até a saída, quais de seus colaboradores ou terceiros têm acesso a eles e a necessidade desse acesso.	1.a. Limite o acesso de colaboradores e/ou funcionários aos dados dos clientes quando esse acesso se mostrar desnecessário. Funcionários de Recursos Humanos, por exemplo, em teoria não precisam ter acesso a dados de clientes.	1.a. Para limitar o acesso de pessoas a dados pessoais de clientes, conte com o auxílio de um profissional de TI – Tecnologia da Informação. Uma alternativa é manter os acessos a dados de clientes somente nos computadores dos colaboradores que realmente necessitam trabalhar com o sistema em que os referidos dados trafegam.
	1.b. Oriente seus colaboradores e/ou funcionários quanto ao	1.b. Elabore um Código de Ética, prevendo as normas éticas em

	manuseio dos dados, exclusivamente para as finalidades definidas pela empresa.	que os colaboradores devem se pautar na execução de seus trabalhos, e um Regimento Interno contendo regras de como os colaboradores devem agir com relação aos dados pessoais de clientes.
	1.c. Impeça o uso de computadores pessoais e/ou celulares de colaboradores e/ou funcionários para fins de trabalho.	1.c. Disponibilize computadores da empresa para a execução dos trabalhos, com todas as medidas de segurança inseridas para impedir o uso incorreto de dados pessoais de clientes e vazamentos. O mesmo deve acontecer com celulares.
2. Liste quais os dados pessoais dos clientes são efetivamente necessários para sua operação.	2. Elimine a coleta de dados pessoais dos clientes que não tenham relevância para o contrato que está sendo firmado.	2. Dados pessoais de clientes desnecessários devem ser excluídos e não devem ser mais coletados. Use, apenas, o necessário para concretizar os contratos.
3. Responda à pergunta "para que estou coletando dados pessoais"? Isso vai definir as medidas que tem que adotar de acordo com cada hipótese prevista na lei.	3.a. Se a resposta à pergunta for "para emissão de boletos e pagamento de tributos"...	3.a. Certifique-se de que os dados sejam usados somente para tal finalidade.
	3.b. Se a resposta à pergunta for "para oferecer novos produtos ou transferir dados para terceiros"...	3.b. Obtenha o consentimento dos clientes para tal ação, ou se certifique de que o condomínio tenha obtido tal consentimento.
	3.c. Se a resposta for "para cumprimento do contrato e posterior contato para oferecer outros produtos, no futuro"...	3.c. No momento da contratação obtenha do cliente documento por escrito informando-o de que os dados serão utilizados para futuros contatos oferecendo produtos, bem como informando que tais dados permanecerão armazenados no sistema da empresa e poderão ser eliminados a pedido do cliente.
4. Liste os programas de computador (softwares) utilizados para coleta e/ou tramitação de dados pessoais de clientes.	4.a. Conte com o auxílio de um profissional da área de Tecnologia da Informação para avaliar se o sistema é seguro com relação à tramitação e proteção de dados de pessoas físicas.	4.a. Se necessário, troque o sistema ou adote medidas diversas para protegê-lo.
	4.b. Se o programa for de empresa terceira...	4.b. Certifique-se de que os computadores da empresa tenham proteções suficientes; certifique-se de que a empresa tenha as proteções necessárias do sistema e esteja providenciando a constante

		manutenção/atualização para evitar brechas/invasões.
5. Liste os sistemas de segurança de informática utilizados nos computadores da empresa (ex.: antivírus, firewall, etc.).	5. Conte com o auxílio de um profissional da área de Tecnologia da Informação para avaliar se o antivírus/firewall é bom e seguro.	5. Se necessário, a depender da avaliação do Técnico em Informática, troque ou atualize o antivírus/firewall.

5) Quais documentos exigidos as empresas devem ter obrigatoriamente?

Outro ponto relevante trazido pela LGPD é a necessidade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais.

Tal relatório consiste na documentação que poderá ser exigida do controlador (profissional liberal, empresa, etc.) pelas autoridades competentes, contendo a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação ao risco.

Em outras palavras, este Relatório deve conter todo o tratamento dispensado aos dados, desde a sua coleta (quando os dados chegam à empresa pelos Bancos ou pelo próprio cliente), o manuseio dos dados (antes e após a realização do contrato), onde ficarão armazenados (servidor, nuvem, etc.), quais os meios para proteção dos dados foram adotados pela empresa, quais os sistemas ou programas de computador são utilizados, etc.

→ Como faço esse Relatório de Impacto?

Reúna, num documento, todas essas informações e aquelas informações da planilha do item 4 desta Cartilha. Além disso, descreva os procedimentos que a empresa adotaria para eliminar dados, se necessário, o contato do Técnico de Informática que conhece o sistema e assessora a empresa nesse sentido.

Indique no relatório quem é o DPO da empresa, aquele profissional que será responsável por assegurar a implementação da LGPD dentro da empresa e dar informações sobre os dados dos titulares.

6) O que acontece se a empresa não se adequar à LGPD?

Da forma como os dados de pessoas físicas são tratados, atualmente, já há risco de vazamentos e uso indevido por pessoas mal-intencionadas. Exemplo disso são os diversos casos que vêm sendo veiculados na mídia e que causaram grandes danos aos titulares dos dados vazados.

Adequar-se à lei, portanto, visa proteger os dados de seus clientes contra danos que um eventual vazamento possa causar.

O vazamento dos dados, em especial envolvendo dados bancários, pode acarretar sérios prejuízos aos titulares/consumidores e, consequentemente, à empresa que não os protegeu adequadamente. E se esses danos se concretizarem, a empresa estará sujeita tanto às penalidades da LGPD como à consequente reparação indenizatória aos titulares.

Uma das penalidades da LGPD é a multa de até 2% do faturamento da empresa ou até R$ 50.000.000,00 por ato que viola a lei, além de outras penalidades cíveis que poderão ser requeridas tanto pela Autoridade competente como pela própria vítima que teve os dados violados, como, por exemplo, o bloqueio das atividades da empresa.

→ Melhores práticas em cibersegurança em adequação à lei geral de proteção de dados

Com a crescente onda de ataques cibernéticos as empresas necessitam tomar medidas preventivas de modo a preservar suas informações. Mais do que isso, normas e legislações vêm sendo estabelecidas em todo o mundo, mas os resultados práticos dependem da conscientização e educação de todos os envolvidos que acessam e manipulam essas informações.

O governo americano, através do NIST (National Institute of Standart and Tecnologies), desenvolveu uma estrutura de segurança cibernética bastante sofisticada que vem sendo aplicada nas organizações de todos os tamanhos e servindo de base para o desenvolvimento de legislações específicas para a cultura de proteção das informações.

O NIST desenvolveu um plano de segurança cibernética visando facilitar seu uso para pequenas empresas, como forma de conscientização da importância de termos noção das informações que produzimos e de como devemos protegê-las e os cuidados que devemos ter ao manuseá-las.

Procuramos resumir um pouco deste plano com o modelo abaixo:

https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

1 – IDENTIFIQUE	
	• Identifique e gerencie todos os equipamentos e dispositivos que acessem a rede corporativa; • Identifique e controle quem acessa as informações corporativas; • Nos processos de contratações, valide as referências e antecedentes; • Mantenha sempre contas de acesso individuais para cada profissional; • Desenvolva, mantenha e treine periodicamente todos os profissionais com relação às políticas de segurança da informação.

2 – PROTEJA	
	• Limite o acesso às informações corporativas; • Instale equipamentos contra variação elétrica e falta de energia (no-breaks); • Mantenha equipamentos, sistemas operacionais e aplicações devidamente atualizados e licenciados; • Instale e mantenha ativos firewalls, tanto programas, quanto equipamentos específicos, para a proteção de toda a rede corporativa; • Adote medidas de segurança para acesso à rede corporativa por meio de redes sem fio ou remota; • Adote filtros de conteúdo de acesso à internet e de envio de e-mails; • Criptografe os dados para o envio de informações sigilosas; • Descarte de forma segura computadores e mídias digitais; • Treine periodicamente seus profissionais, principalmente com assuntos relacionados à segurança da informação.

3 - DETECTE	
	• Instale e atualize programas de antivírus, antimalware, etc.; • Mantenha e monitore os registros de atividades da rede (Logs); • Monitore periodicamente as atividades de acesso à internet; • Acompanhe painéis de monitoramento de antivírus ou outras ferramentas de detecção e prevenção de ataques; • Acompanhe periodicamente informativos de atualizações de emergência contra o ataque de vírus.

4 - RESPONDA	
	• Desenvolva um plano de respostas a incidentes e desastres; • Papéis e Responsáveis; • Procedimentos a serem realizados; • Quem acionar em caso de incidentes; • Atividades que representam um incidente de segurança.

5 - RECUPERE	
	• Mantenha backup integral de todas as informações dentro e fora da empresa, de preferência criptografado; • Avalie contratar um seguro de responsabilidade civil ou contra os ataques cibernéticos; • Mantenha avaliações constantes de modo a implementar melhorias em processos, procedimentos e nas tecnologias utilizadas.

A base de todo o processo de segurança cibernética está em estabelecer um processo contínuo de manutenção do ambiente de TI. De pouco adianta investir uma única vez e não efetuar a manutenção dos equipamentos e do treinamento contínuo dos profissionais.

As novas legislações exigem a documentação e comprovações com evidências de todos os procedimentos e cuidados realizados para se manterem as informações seguras e os acessos efetuados às redes, bancos de dados e sistemas. Sem estas comprovações e evidências, a empresa estará sujeita a sanções previstas na lei pelos órgãos reguladores.

Procure estabelecer processos e padrões que garantam esta regularidade e manutenção de todos estes itens de forma sistemática.

Referências Bibliográficas:

https://www.nist.gov/

https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

https://www.nist.gov/itl/smallbusinesscyber

https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

https://www.restaurant.org/Downloads/PDFs/advocacy/cybersecurity101.pdf

https://www.stopthinkconnect.org/

https://www.escolavirtual.gov.br/curso/153

https://www.serpro.gov.br/lgpd/menu/a-lei/o-que-muda

https://politica.estadao.com.br/blogs/fausto-macedo/como-se-prevenir-e-evitar-perda-ou-vazamento-de-dados-na-internet/?utm_source=estadao:whatsapp&utm_medium=link

https://www.cert.br/

https://internetsegura.br/

http://www.familiamaissegura.com.br/