LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

LGPD SIMPLIFICADA

Os textos descritos neste material não têm a finalidade de ser um orientador sobre como proceder com a adequação da empresa à LGPD.

O objetivo é passar às pessoas que ainda não tiveram a oportunidade de se aprofundar no assunto, ou aos empresários e gestores, uma linguagem mais comum, sem termos técnicos ou jurídicos, sobre o que é a LGPD e como isso pode ser visto dentro da empresa.

Por ser uma lei, a interpretação jurídica é sempre o primeiro caminho, mas não o único.

Vamos tentar, com uma linguagem mais simples do dia a dia passar as necessidades que precisarão ser previstas e atendidas.

CONTEXTUALIZAÇÃO

Você, empresário ou gestor, já deve ter ouvido falar sobre a LGPD, a Lei Geral de Proteção de Dados.
E já deve ter recebido diversos retornos, provavelmente com algum embasamento jurídico sobre o que se trata.
Isso não está errado pois estamos falando de uma lei e ninguém mais indicado que um advogado para responder.
Caso ainda não saiba do que se trata ou ainda não evoluiu com o assunto, é bom começar a pesquisar e se preocupar.

A LGPD

Por ser lei, tem dois fatores principais que precisam ser observados:

O primeiro é que normalmente se consulta o jurídico para entender do que se trata.

O segundo é que por ser uma lei, apesar de algumas interpretações diferentes sobre alguns parágrafos, é unanimidade que precisa ser atendida na sua integralidade.

E quem não cumprir estará sujeito a multas e sanções administrativas.

Falando com termos mais comuns, a LGPD diz que **cabe a quem faz a coleta e o tratamento (uso) dos dados das pessoas, a responsabilidade de proteger a privacidade destes dados.**

Simples e ao mesmo tempo complexo.

Vamos, nesta mesma linha mais comum, sem termos jurídicos ou técnicos, definir um pouco do que precisará ser feito e quais as consequências caso a proteção a privacidade dos dados seja quebrada.

COLETA DE DADOS

E o que vem a ser a “coleta dos dados”?

Qualquer operação de obtenção de dados de pessoas físicas (coleta de dados de pessoas jurídicas não se enquadram no contexto da lei) que tenham como objetivo o uso para uma determinada finalidade. A responsabilidade vale tanto para empresas privadas como públicas.
Note para um detalhe da frase, que diz “uso para **UMA** determinada finalidade".

Finalidade

Como exemplo, para ficar mais claro, vamos pegar uma empresa do setor de construção civil. Esta empresa constrói e vende apartamentos. Para atender aos agentes de venda, monta stands em determinados locais. Esses agentes “coletam” dados de pessoas interessadas na aquisição de um apartamento. Dentre essas pessoas, algumas viram clientes e compram o imóvel, outras simplesmente não retornam ou não manifestam interesse.
Isso refere-se a uma operação de coleta e tratamento de dados de pessoas físicas, com a FINALIDADE de gerar, por exemplo, um contrato de compra e venda de apartamento.
E, nesse caso, a coleta de dados pode conter dados do interessado, do cônjuge e também de DOCUMENTOS, como comprovantes de residência, Imposto de Renda, etc.
Fica, portanto, evidenciado que a coleta pode ser de dados lógicos como também de documentos físicos e o procedimento de proteção a privacidade deve ter o mesmo critério.
Sem aprofundar muito no que diz a LGPD para facilitar o entendimento, esses dados coletados SOMENTE podem ser utilizados para a FINALIDADE da coleta.

Antes de seguirmos, vamos a uma situação de grande importância e que precisará, com base neste exemplo e que pode ser retratado para uma situação real, ser tratado.

Temos duas situações: Uma de pessoas interessadas que viraram clientes e outra de interessados que desistiram. De qualquer maneira, independente do desfecho de cada interessado, isso configura uma operação de tratamento de coleta de dados.

Com base no que foi citado, tratamentos distintos devem ser seguidos.
Primeiro: Os interessados que não viraram clientes. O que a construtora pode fazer com esses dados coletados? A resposta é NADA, a não ser eliminar, a menos que no processo de coleta o interessado (potencial cliente) tenha se manifestado formalmente que deseja permanecer na base de dados para futuros novos lançamentos ou vendas.
Segundo: Os interessados que viraram clientes. Isso é uma nova Operação de tratamento de dados e todos os cuidados previstos na LGPD devem ser seguidos, tendo como parâmetro o processo de adequação realizado.

Aí alguém de marketing pode perguntar: “Mas como fazer para divulgar novos empreendimentos se não pode manter a base de interessados?”.
Essa é uma resposta que o jurídico, junto com a equipe multi disciplinar poderá responder e, se possível, encontrar uma forma de uso prevista na lei. Caso contrário, o mais prudente será eliminar.

E essa construtora, durante o período de construção pode fazer uso desses dados para ofertar móveis planejados, por exemplo?

A resposta é, a princípio, NÃO. E por que a princípio NÃO? Porque pela lei os dados somente podem ser utilizados para a FINALIDADE indicada na coleta, que é a produção de um contrato de compra e venda.

Quando isso pode gerar a possibilidade do NÃO?

Quando, no momento da coleta, o titular que estiver informando seus dados, CONSENTIR formalmente que concorda em receber esse tipo de comunicado.

Ressaltando que não basta um consentimento genérico. Precisa ser explícito cada nova possibilidade de uso destes dados. Todas essas operações de tratamento, para este exemplo onde foi solicitado um consentimento adicional, também precisam ser registradas conforme o disposto na lei.

Anteriormente falamos que proteger a privacidade dos dados era simples e ao

mesmo tempo complexo.
Dá para perceber que é simples, pois basta seguir os procedimentos, mas é complexo porque são muitas possibilidades para serem pensadas.
Seguindo este mesmo exemplo e raciocínio, os agentes de vendas podem ter feito o registro desses interessados (que viraram clientes ou não) em planilhas (o que é bastante comum) e estas planilhas estão gravadas no notebook de cada vendedor que, ao final do dia, enviam para a sede da construtora inserir as informações nos sistemas.

Como o objetivo da LGPD é proteger a privacidade dos dados dos titulares, fica claro que existe um RISCO muito grande para ser analisado, pois os agentes podem continuar com os dados nas suas planilhas. E quem garante que um agente de vendas use estes dados para passar para um amigo que tem como cliente este mesmo público?
Sabe de quem é a responsabilidade? Da construtora. E sabe quem será autuado? A construtora. Veremos adiante, com base nesse exposto, a necessidade de treinamento contínuo e conscientização de responsabilidades e implicações em caso de negligência.

Deu para perceber que além de se preocupar internamente em usar os dados apenas para a finalidade de coleta precisa se preocupar também com esses usos indevidos?
E, se por força do negócio, seguindo o exemplo da construtora, for necessário compartilhar esses dados com alguma outra empresa. Isso é possível e contemplado pela LGPD?
SIM, é possível e é contemplado pela LGPD. Porém existem regras bem claras de como isso pode e deve ser feito. Precisa ser algo formal (com embasamento jurídico em contratos), controlado e totalmente documentado podendo, inclusive, ser necessário o consentimento do titular para que o compartilhamento seja realizado.

O objetivo não é causar terrorismo, mas expor de maneira clara, numa linguagem bem prática que a situação não pode e não deve ser negligenciada e procastinada.

E isso é apenas uma pequena, bem pequena, parte do que precisa ser atendido com a LGPD.

Para pensar!

Para pensar, algumas determinações da LGPD:

1 – TODA empresa que de alguma maneira coleta e faz tratamento de dados de pessoas físicas está enquadrada na lei. NÃO existe, até o momento, nenhuma isenção.

2 – TODA empresa precisa nomear um "Encarregado de Proteção de Dados". E designar "alguém de TI", ou "algum diretor" sem critério e formação adequada pode resultar em risco de sanções administrativas e financeiras.

3 – É uma BOA PRÁTICA montar uma equipe multi disciplinar, envolvendo no mínimo o jurídico, segurança da informação e tecnologia da informação.

4 – A empresa precisa disponibilizar um CANAL DE COMUNICAÇÃO para que os titulares dos dados possam registrar suas solicitações.

5 – Tentar montar toda a estrutura de adequação à LGPD por conta própria, sem contar com uma consultoria especializada pode gerar custos elevados e por em risco o processo de adequação. Não por incapacidade de eventual equipe, mas por falta de tempo e foco, pois num momento de decidir entre uma reunião sobre a LGPD e sobre um tópico interno, o tópico interno, na maioria das vezes, será priorizado.

6 – PRECISA ter treinamento para todos os funcionários e precisa ficar EVIDENCIADO quem foi treinado alem de uma periodicidade de revisão desses treinamentos. Lembre-se do caso citado anteriormente do agente de vendas que pode usar os dados coletados de interessados e passar (mesmo que sem segundas intenções) para um amigo. Isso configura vazamento ou acesso indevido aos dados e é passível de multa financeira e/ou sanções administrativas.

7 – NÃO questione se a lei vai pegar ou não vai pegar e, com base nisso, deixar acontecer para ver o que fazer. A LGPD é uma lei que foi sancionada pelo governo federal com todas as fases jurídicas plenamente cumpridas.

8 – A partir de agosto de 2021 as empresas estarão sujeitas às sanções administrativas e financeiras, com multas que podem chegar a 50 milhões de reais.

EXEMPLOS

Alguns exemplos que podem ajudar a entender a lei e suas responsabilidades.

RECRUTAMENTO E SELEÇÃO

- Toda empresa, em algum momento, precisa contratar funcionários.
- E para isso existe um processo de recrutamento e seleção onde candidatos se inscrevem para uma vaga e participam do processo.

Recrutamento e Seleção

Ao se inscrever para um processo o candidato deve, através de um portal ou por meio físico, informar seus dados pessoais. E, ao fazer isso de maneira voluntária, está autorizando o uso desses dados para a finalidade de “recrutamento e seleção". Essa informação de finalidade deve (como sugestão), inclusive, ficar destacada para evitar qualquer problema de interpretação.

Além é claro, de um termo jurídico de consentimento destacando a necessidade de informação dos dados e as consequências caso esse consentimento não seja formalizado.

A empresa responsável pela coleta pode fazer uso desses dados para enviar, por exemplo, um e-mail com oferta de algum produto ou serviço?

Não, não pode.

Se mandar e a pessoa se sentir prejudicada poderá registrar uma reclamação?

Sim, poderá.

E a empresa, por esse motivo, poderá ser multada? Sim, poderá.

E o que fazer com os cadastros dos candidatos que não foram selecionados?

Aí poderá depender de uma interpretação jurídica para avaliar o modelo como os dados dos candidatos foram coletados para definir qual procedimento utilizar. Como a FINALIDADE da coleta de dados foi a de recrutamento e seleção, caso esses dados sejam mantidos na base não deverá haver quebra de finalidade se novos contatos forem para recrutamento e seleção.

Precisa ficar muito evidente que um acompanhamento jurídico é importante para que os processos sejam corretamente fundamentados além da LGPD, nas diversas leis já existentes, como Código de Defesa do Consumidor, Código Civil, Estatuto da Criança e Adolescente, etc.

A indicação da possibilidade de análise de uma equipe multi disciplnar é quanto ao RISCO de ocorrer um acesso indevido ou vazamento contendo esses dados dos candidatos não selecionados. Como todo RISCO, ao ser tratado, caberá aos gestores a decisão quanto ao procedimento a ser adotado.

AGÊNCIA DE VIAGENS

- Você, pessoa física, decide fazer uma viagem de férias com a família. Supondo que para facilitar todo o processo, vá até uma agência de viagens.

Agência de Viagens

Na agência, ao falar com o atendente, você declara seu desejo para uma viagem para um local qualquer que, para ser realizado dependerá de reserva de passagem aérea e hospedagem.

Nesta viagem irá você, o cônjuge e dois filhos, um de 18 e outro de 16 anos.

Sem entrar muito no contexto específico da lei, e para simplificar o exemplo, você precisará fornecer os seus dados, do cônjuge e dos dois filhos para que a agência possa providenciar a reserva das passagens e da hospedagem.

A agência neste caso está fazendo a coleta dos dados e COMPARTILHANDO com as demais interessadas, até mesmo para que o objetivo seja alcançado.

A interpretação da lei, neste caso, pode gerar desdobramentos diferentes (para os mais experientes e conhecedores do assunto, quem é o Controlador, quem é Operador, etc.). Mas vamos pelo caminho de entendimento de uma maneira mais simples.

Caso o formulário de preenchimento dos dados dos viajantes ainda não contemple os atendimentos sobre a LGPD, este formulário precisará ser modificado para que o titular manifeste **formalmente** e para cada **necessidade** (passagem aérea, hotel, etc.) que **CONCORDA** que seus dados sejam compartilhados.

Neste exemplo outros desdobramentos devem ser previstos.

Como a FINALIDADE da coleta dos dados foi para uma viagem, a lei cita que quando a FINALIDADE for cumprida o responsável pela coleta deve ELIMINAR os dados. Esse desdobramento pode suscitar entendimentos diferentes sobre a manutenção dos dados, se deve e, caso positivo, como eliminar. Quanto tempo tem para executar?

Por esta linha de raciocínio, a agência de turismo deve ter procedimentos que validem cada registro de viagem para que, ao término de cada viagem, os dados referentes sejam eliminados e, consequentemente, as empresas que receberam esses dados também devem executar esse mesmo procedimento de eliminação.
Aí então alguém pode perguntar: Mas como controlar isso?
Como fazer para avisar as demais empresas que dados precisam ser eliminados?
Cabe, no momento das atividades de adequação à LGPD, definir como isso será feito.

E se não for feito, quais os riscos envolvidos e como serão tratados.

Lembrando ainda que a LGPD prevê uma série de direitos aos titulares dos dados, estando previsto nestes direitos, a solicitação de eliminação.
Dessa forma, como veremos adiante, a empresa deve disponibilizar canal de comunicação para que os titulares possam registrar suas solicitações de direitos previstos na LGPD.

ACESSOS

Acessos são controles lógicos e físicos que permitem a gestão de usuários, clientes, terceiros, no ambiente da empresa.

Acessos lógicos estão relacionados aos sistemas e acessos físicos, a catracas, portas, etc.

ACESSOS

- Violação de acessos, como deve ser entendido?
- Internos e Externos.
- Acessos indevidos por mudança de posição ou por desligamentos.
- Em afastamento ou férias, como controlar os acessos?

Acessos

Naturalmente quando perguntado sobre violação de acessos o que vem primeiro a mente como resposta é referente a invasão de hackers. Ou seja, a empresa está devidamente protegida contra esses eventuais ataques?

Essa preocupação é totalmente pertinente e não pode ser deixada de lado nunca. Mas, quando o assunto é ACESSOS, é fundamental tratar também os acessos internos, ou seja, na equipe de colaboradores e terceiros, como é que está esta gestão?

A LGPD cita também a atenção que deve ser direcionada aos acessos para que determinado colaborador (ou terceiro) SOMENTE possa ter acesso nos sistemas às telas ou informações que são pertinentes a esse colaborador.

Dessa maneira, por exemplo, um colaborador do RH deve ter acesso às telas do RH, assim como um colaborador do financeiro somente pode ter acesso às telas financeiras e assim deve ser validado para todos que, de alguma maneira, tenham acesso aos sistemas.

Pode parecer simples, mas a execução manual dessa gestão demanda muito trabalho. E trabalho que cai sobre a responsabilidade da equipe de T.I., que normalmente está sobrecarregada com outras demandas e faz o que é possível dentro da capacidade.
Vamos além.....
Quem é que sabe, na empresa, quais são esses acessos que precisam ser concedidos quando um novo funcionário é contratado? RH? T.I.? O gestor da área? Quem?
Por incrível que possa parecer essa preocupação não existia até então. Muitas vezes a instrução era de pegar um perfil semelhante e copiar. Só que agora gestão de acessos é uma das regras básicas para a LGPD!
E, mais crítico ainda, é quando um colaborador é demitido e continua com os acessos vigentes.
Ou ainda, um colaborador em período de férias com acesso aos sistemas, e-mail, etc. Se for o presidente da empresa, pode continuar com acesso quando em férias. Se puder, o que poderá acessar?
Dentre vários riscos envolvidos, acessos a sistemas em período de férias pode configurar atividade de trabalho e "render" uma reclamação trabalhista.

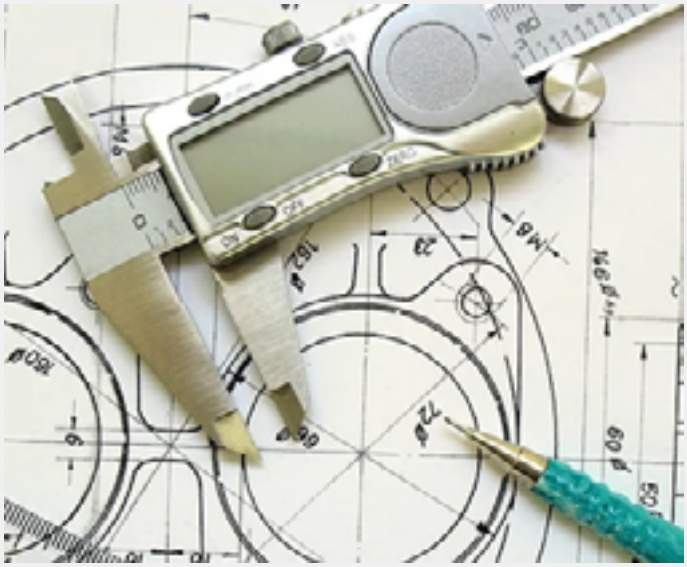
Sobre os acessos:
1. A empresa possui processos de ONBOARDING e OFFBOARDING?
2. Quanto tempo demora para a concessão dos acessos?
3. Quando um colaborador for promovido, como será a definição dos novos perfis? E os antigos?
4. Existem evidências para auditoria? Quem tem essa informação para apresentar quando solicitado?
5. Como é o controle dos acessos para pessoas em home office?

RISCOS

Independente da LGPD, RISCOS existem, estão presentes em todas as organizações e devem ser identificados e tratados, conforme a gravidade.

RISCOS

- Identificar e tratar os riscos faz parte do processo de adequação.
- Quem consegue identificar quais são os riscos no processo?
- Classificação dos riscos de acordo com a relação de probabilidade x impacto.



Riscos

A LGPD trouxe à tona com mais intensidade este tema pois para proteger a privacidade dos dados dos titulares e entender como a organização trata isso, identificar os riscos e impactos passa a ser fundamental para atingimento do sucesso.

Isso significa que todos os riscos devem ser eliminados?

No mundo ideal a resposta seria positiva, mas se fizermos uma análise mais profunda, sequer é possível identificar todos os riscos, quanto mais eliminar a todos!

É óbvio que isso não serve de desculpa em momento algum, muito menos com a LGPD.

Quem está no dia a dia da empresa, na operação, sabe identificar grande parte desses riscos e tem condições, inclusive, de propor maneiras de, ao menos, mitigar esses riscos.

Se temos condição de identificar quais são os riscos e ter propostas que podem eliminar ou mitigar, por que não fazer isso?

Será que algum dia alguém teve a iniciativa de fazer esse questionamento?

Não é a LGPD que obriga ninguém a fazer isso, pois no dia a dia e na necessidade de fazer “tudo para ontem”, muitos riscos são ignorados.

Riscos não são apenas financeiros, que podem fazer a empresa perder faturamento, atrasar recebimentos, pagar juros por inadimplência.

Alguém já pensou no risco reputacional? Quanto vale a reputação de uma empresa?

Quanto pode custar, tanto financeiro quanto reputacional, se um dado coletado for vazado, copiado e distribuído indevidamente, utilizado de forma equivocada (proposital ou não)?

Quanto a imagem (reputação) de uma empresa pode ficar abalada se um colaborador mal treinado ou mal intencionado fotografar informações sensíveis e publicar nas redes sociais?

Processos relativamente simples e muitas vezes ignorados devem ser analisados para, além da definição das atividades, ser possível também identificar os riscos.

O objetivo não está relacionado a maneira como os riscos e impactos devem ser tratados, mas ficar evidenciado que é extremamente importante o conhecimento que existem riscos e seus impactos, tanto para a empresa como para o titular.

SOLICITAÇÕES DOS TITULARES

A LGPD institui diversos direitos aos titulares que devem possibilitar um relacionamento mais próximo entre os titulares dos dados e a empresa.

E cabe a empresa prover e promover esse canal de comunicação, assim como atender a todos os requisitos e prazos definidos na lei.

Muitas dessas solicitações dos direitos podem e deverão envolver diversos setores dentro da empresa, dentre os quais, jurídico, segurança da informação, tecnologia da informação.

SOLICITAÇÕES DOS TITULARES

- Deve ser simples, fácil e sem custo.
- Tem prazo para resposta.
- Sujeito a multas financeiras e administrativas.
- Deve gerar evidências.

Atendimento das Solicitações dos Titulares

Disponibilizar o já conhecido “Fale conosco” nos web sites das empresas é algo comum e amplamente utilizado como um meio de comunicação para que os clientes ou interessados possam registrar seus desejos ou esclarecimentos. Mesmo que em muitos casos o “Fale conosco” tenha um direcionamento, nem sempre quem fez o registro recebe uma resposta ou qualquer retorno.

Com a LGPD essa responsabilidade é totalmente diferente dos simples formulários de “Fale Conosco”.

O titular dos dados, seja ele cliente, terceiro, funcionário, etc., tem seus direitos definidos com regras e prazos para atendimento.

Protocolo de atendimento: Toda solicitação precisa ter um controle que informe ao titular esse número ou qualquer outra informação que faça referência ao registro.

Prazo para atendimento: O prazo máximo para retorno é de 15 dias, a princípio, como definido na lei, sem possibilidade de a empresa solicitar prorrogação.
Canais de comunicação: A empresa precisa criar e divulgar esses canais de comunicação para que as pessoas, independente de possuírem algum registro de cadastro, possam solicitar informações. E sempre terá que haver uma resposta encaminhada ao solicitante.

Simplificando, cabe a empresa criar e disponibilizar meios para que qualquer pessoa possa registrar uma solicitação, com um prazo de resposta nunca superior a 15 dias.
E, segundo a lei, deve ser por meio simples, fácil e sem custo.

E o que acontece se não houver uma resposta ou se ultrapassar os 15 dias definidos na lei?
O solicitante poderá registrar queixa nos órgãos competentes (Autoridade Nacional de Proteção de Dados, PROCON, e outros que serão designados) e a empresa deverá responder por essa negligência, sujeita a multas, sanções administrativas e até indenização.
Uma outra situação que precisa ficar bem clara e evidenciada é que o titular pode registrar quantas solicitações forem necessárias para que suas dúvidas ou requerimentos sejam atendidos e cabe à empresa receber e responder a todas sem maiores questionamentos ou justificativas.
Muito provavelmente as empresas não possuem dados históricos para medir o esforço que será necessário para atendimento das solicitações. Nem mesmo quantas solicitações poderão ser registradas por dia, por mês, etc.
Mas dá para prever que será um problema. Primeiro: Como receber e registrar?
Segundo: Quem vai receber?
Terceiro: Quem vai tratar?
Quarto: Quem vai se responsabilizar por coordenar o que precisará ser feito?
Quinto: T.I. terá que ser envolvida na grande maioria dos casos. Tem pessoal suficiente para as tarefas do dia a dia e atendimento dessas novas solicitações?
Se forem registradas 10 solicitações num mês, qual o impacto no dia a dia da empresa? E se forem 20, 30, 100?

TREINAMENTO

Tão importante quanto entender e mapear os processos, vulnerabilidades, riscos, definir as políticas, é TREINAR as pessoas que de alguma maneira acessam ou manipulam qualquer tipo de dado pessoal.

TREINAMENTO

- Tema recorrente para diversas situações da empresa.
- Deve-se gerar evidências e montar um plano de
- treinamento.
- Cuidados com a perda de conhecimento com a demissão de funcionários treinados.

Atendimento das Solicitações dos Titulares

De nada adianta investir milhões num super equipamento se não tiver pessoal treinado para operar.
De nada adianta investir pesado na adequação à LGPD se todas as pessoas que podem ter qualquer tipo de acesso aos dados também não estiverem treinadas.
Dentre as diversas necessidades que precisarão ser atendidas para a adequação à LGPD está a elaboração de um Plano de Treinamento.
Muito tempo e dinheiro serão investidos nos mapeamentos dos dados, processos, revisão de contratos, etc. E tudo isso poderá ser inútil se as pessoas que forem acessar e manipular dados (lógicos ou físicos) não souberem as responsabilidades impostas pela LGPD.
Cabe a empresa promover esses treinamentos para a capacitação dos funcionários e terceiros. E garantir o registro das evidências sobre esses treinamentos realizados, de preferência com o registro dos participantes pois caso algum processo seja quebrado e os dados de titulares usados indevidamente, seja possível demonstrar a predisposição de preparar e instruir quanto aos cuidados que devem ser tomados.
Deve-se levar em consideração também o fato de ter que revisar os treinamentos com base nos feedbacks dos treinandos e promover a melhoria contínua.
Outro fator importante a ser considerado é quanto a troca de pessoas na empresa, seja por demissão, promoções, etc.
Esse conhecimento precisará ser constantemente revisado e passado para as pessoas, mesmo que nenhuma troca de pessoal tenha acontecido, pois o dia a dia acabará gerando descuidos que poderão ser graves e resultar em multas.

SEGURANÇA DA INFORMAÇÃO

Política de Segurança da Informação é um conjunto de definições / políticas emitidas por uma organização para garantir que todos os usuários tenham conhecimento sobre o uso e acesso aos sistemas e dados que de alguma maneira manipulam.

Tem por objetivo possibilitar o gerenciamento

da segurança em uma organização, estabelecendo regras e padrões para proteção da informação, no contexto da LGPD, para a proteção à privacidade dos dados dos titulares.

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

- Em algum momento Segurança da Informação foi prioridade?
- Simplesmente definir uma Política de Segurança da Informação será suficiente?
- Minha equipe interna possui capacitação para definir a PSI?
- Existem riscos por falha na definição da PSI?

Segurança da Informação

Esse tema não é tão comum entre as empresas, mesmo aquelas mais avançadas em quesitos de segurança.

E, podemos criticar o empresário ou os gestores por não terem dado atenção para esse quesito?

Sendo coerente, e tendo como base as estratégias das empresas brasileiras, investir em política de segurança da informação nunca foi prioridade.

Agora é ou pode ser prioridade?

Com a LGPD, pelo menos definir uma Política de Segurança da Informação e tornar público essas políticas passa a ser fator fundamental para os processos de adequação.

Se essa política será seguida, vai depender do quanto a alta direção estiver comprometida, não só com a definição, mas com o cumprimento daquilo que for definido.

Dá para fazer essa definição com minha equipe interna, eventualmente "aproveitando" alguns funcionários?

Difícil, muito difícil.

Assim como muitas outras exigências operacionais da empresa que demandam especialistas, a definição da PSI também demanda. E, ao menos que na equipe tenha esse especialista, a chance de sucesso é mínima. Não adianta se enganar, o item é fator de sucesso!
São necessários métodos, procedimentos, conhecimentos, boas práticas para que uma PSI seja eficiente e, somente um profissional no assunto pode dar o retorno desejado.

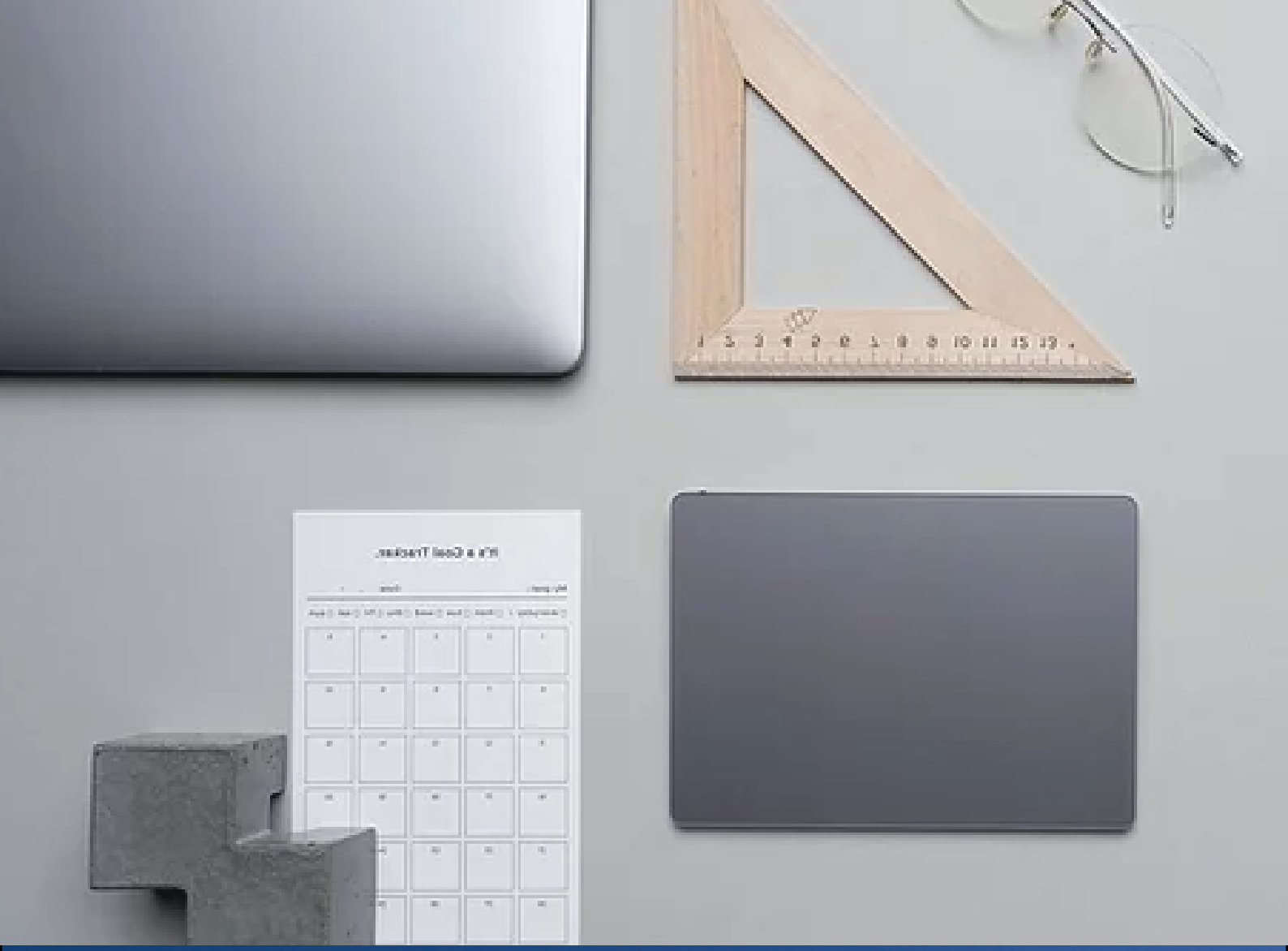
Por exemplo: Você, empresário ou gestor, confiaria a definição ou revisão de um contrato a alguém que não seja da área jurídica e especialista no assunto?
Muito provavelmente não, pois isso poderia acarretar prejuízos financeiros, riscos reputacionais, etc.
Esse especialista poderia escrever uma PSI?
Não, porque a especialidade e necessidade é outra. Cada qual com seu conhecimento e capacidade para cada tarefa.

Seguindo por essa linha de raciocínio, com um especialista em PSI para escrever tudo o que precisa. Isso será suficiente para a adequação à LGPD?
Será se, após escrita e revisada, todos os envolvidos com os processos da empresa que de alguma forma possam ser afetados pelas definições na PSI, forem devidamente treinados e seguirem o que foi definido.
Mas como garantir isso? Investir na contratação para escrever a PSI e depois ainda correr o risco de ficar com um documento guardado na gaveta de um armário?

Como agravante ainda tem o fato do treinamento ser perdido pelo desligamento (algo normal) de funcionários ou terceiros.

Vamos aos fatos:
A PSI precisa ser escrita para a adequação à LGPD. Precisa ter um especialista para definir e escrever. Precisa ter treinamento de funcionários e terceiros. Existe o risco de perda de conhecimento.

A saída pode ser:
- Conviver com o risco e assumir que existe a possibilidade de multas e sanções administrativas.
- Estruturar a PSI em tópicos controlados por um sistema de adequação à LGPD que permita o monitoramento dos itens através de robôs ou procedimentos de checagem disparados periodicamente para determinados gestores.



CONCLUSÃO

CONCLUSÃO

A Lei Geral de Proteção de Dados é lei, sancionada e vigente, que deve ser atendida por todas as empresas, não importa o tipo, tamanho, faturamento ou número de funcionários, seja ela pública ou privada, desde que haja tratamento de dados de pessoas físicas.

Foi concedido um período de 24 meses, desde a aprovação da lei (13.709/18), para que as empresas pudessem se planejar técnica e financeiramente para a adequação sem que as multas fossem aplicadas. Prorrogações nesse prazo foram concedidos e a partir de agosto de 2021 as multas começarão a ser aplicadas.

O impacto de uma não adequação à LGPD ou uma adequação incompleta poderá gerar conflitos comerciais entre empresas (tanto nacionais quanto internacionais) pois uma empresa devidamente adequada deverá revisar seus contratos com as empresas parceiras visando garantias no tratamento dos dados compartilhados.

Muito provavelmente as empresas que não estiverem adequadas à LGPD terão dificuldades de comprovar como estão protegendo os dados dos titulares.

Tentar fazer tudo por conta própria sem que hajam especialistas no processo é extremamente arriscado.

Nomear o Encarregado de Proteção de Dados sem que essa nomeação seja de um profissional conhecedor do tema LGPD poderá gerar um falso positivo pois na hora que precisar, a falta de conhecimento da lei e como deve ser o relacionamento com os titulares ou Autoridade Nacional de Proteção de Dados, poderá resultar em multas.

A adequação à LGPD é um processo contínuo, que demandará constantes análises e atualização das informações. Dessa forma, gerar documentos e guarda-los no armário não será suficiente.