IPEEA

CAMARGO & VIEIRA
SOCIEDADE DE ADVOGADOS

Guia de adequação:

A Lei Geral de Proteção de Dados para entidades de Engenharia e Agronomia

Índice

1. O que é a Lei Geral de Proteção de Dados?

A Lei Geral de Proteção de Dados Pessoais – LGPD – regula o tratamento de dados pessoais.

Ela tem como objetivo fomentar o desenvolvimento econômico e tecnológico das empresas e proteger os dados, direitos e liberdades individuais dos titulares

Esta cartilha apresenta um panorama sobre a Lei 13.709 de 2018, para que as **associações filiadas ao Instituto Paulista de Entidades de Engenharia e Agronomia (IPEEA) tomem conhecimento sobre a importância do tema** e comecem a adotar algumas medidas que possam preservar os dados utilizados em suas atividades.

2. Definições

DADO PESSOAL - É qualquer informação que identifica ou pode identificar uma pessoa, como nome, endereço, perfil online, e-mail, contatos, empresa onde trabalha, endereço de IP, CPF, RG, número de telefone, códigos de identificação (Cookies), etc.

DADO PESSOAL SENSÍVEL – São dados que, pela sua sensibilidade natural, podem levar o titular a situações discriminatórias, por isso possuem uma proteção extra pela lei. São dados de uma pessoa natural relacionada à origem racial ou étnica; saúde ou vida sexual; genética e biometria; filiação a sindicato; convicção religiosa; e opinião política.

DADO ANONIMIZADO – Dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

PSEUDOANONIMIZAÇÃO – Quando a empresa separa os dados de forma que os funcionários só têm acesso a alguns dados, não conseguindo identificar o titular. Contudo, é possível reverter o processo, pois a empresa é detentora dos dados.

TRATAMENTO – É tudo aquilo que pode ser feito com um dado pessoal durante a realização de uma atividade, como coleta, registro, acesso, uso, transferência, armazenamento, compartilhamento e exclusão.

CONTROLADOR - É a pessoa que decide como, quando e por quê tratar os dados pessoais. Essa pessoa pode ser natural ou jurídica, de direito público ou privado.

AGENTES DE TRATAMENTO - São assim denominados o controlador e o operador.

OPERADOR - É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador. Importante lembrar que um funcionário nunca será considerado um operador, mas sim a entidade que ele representa.

TITULAR DE DADOS – Pessoa natural a quem os dados tratados se referem.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) – Órgão responsável pela fiscalização, educação, regulamentação e monitoramento do cumprimento da LGPD.

ENCARREGADO – É a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e ANPD.

3 Em quais situações a LGPD é aplicável?

Vigente desde 2018, a LGPD se aplica toda pessoa física, jurídica e órgãos da administração pública que realize tratamento de dados dentro do território nacional, que ofereça serviços no Brasil ou que utilize dados de brasileiros.

Inicialmente, é importante ressaltar que a lei se aplica independentemente se o tratamento de dados é realizado **dentro ou fora da internet**, utilizando ou não meios digitais como, por exemplo, formulário em papel, contratos etc.

Contudo, a lei não se aplica quando o tratamento de dados possuir alguma das seguintes finalidades:

- Particular;
- Jornalística;
- Artística;
- Acadêmica;
- Segurança Pública;
- Defesa Nacional;
- Segurança do Estado;
- Atividades de investigação e repressão de infrações Penais.

Assim, utilizar dados pessoais para elaborar contratos, armazenar formulários de admissão de funcionários e enviar e-mail marketing para possíveis clientes/associados são exemplos de atividades que devem observar as normas apresentadas pela LGPD.

4. Os princípios da Lei Geral de Proteção de Dados

1 **Finalidade**
O tratamento dos dados pessoais deve ser realizado para propósitos legítimos e específicos informados explicitamente ao titular.z

2 **Adequação**
O tratamento dos dados pessoais deve ser compatível com as finalidades informadas ao titular.

3 **Necessidade**
Os dados pessoais utilizados devem ser limitados ao mínimo necessário para atingir a finalidade, devendo os dados serem pertinentes, proporcionais e essenciais para a atividade.

4 **Qualidade dos dados**
Os dados devem sempre estar corretos, atualizados, claros e serem relevantes para a finalidade buscada por meio do tratamento.

5 **Livre acesso**
Aos titulares deve ser garantida a consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como o acesso à integralidade dos dados tratados.

6 **Transparência**
As informações sobre como o tratamento é realizado, quais dados são utilizados e quais são os agentes envolvidos nos processos devem ser claras e acessíveis.

7

Segurança

Necessidade de se buscar medidas técnicas e administrativas seguras para proteger os dados pessoais tratados a fim de minimizar possíveis dados de incidentes de segurança internos ou externos, sempre levando em conta o porte da empresa.

8

Prevenção

Buscar medidas internas a fim de evitar a ocorrência de danos às pessoas naturais em virtude do tratamento dos seus dados, como possuir um programa de governança em privacidade e proteção de dados, cartilhas e treinamento de funcionários.

9

Não discriminação

Os dados tratados não podem ser utilizados para fins discriminatórios.

10

Responsabilização e prestação de contas

Os agentes devem ser capazes de demonstrar que medidas eficazes em relação à proteção de dados foram adotadas a fim de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, principalmente no caso de um incidente de segurança ou diante de uma solicitação da Autoridade Nacional de Proteção de Dados.

5 Quando a lei permite o uso de dados?

Para o cumprimento de obrigação legal ou regulatória pelo controlador;

Para a realização de estudos por órgão de pesquisa, que tenha em seu objeto social a finalidade de pesquisa científica, histórica, tecnológica ou estatística;

Mediante o consentimento livre, específico, inequívoco e expresso do titular dos dados pessoais;

Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

Para o exercício regular de direito em processo judicial, administrativo ou arbitral;

Quando necessário para atender aos interesses legítimos do controlador ou de terceiros;

Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Para a realização de estudos por órgão de pesquisa, que tenha em seu objeto social a finalidade de pesquisa científica, histórica, tecnológica ou estatística;

Para realização de políticas públicas pelos órgãos da administração direta ou indireta.

6. Penalidades

Caso alguma empresa não cumpra as normas previstas na LGPD, elas estarão sujeitas a uma **série de penalidades que podem ser aplicadas pelas ANPD**, como:

- Advertência;
- Publicação da infração;
- Bloqueio ou eliminação dos dados pessoais a que se refere a infração;
- Suspensão do exercício da atividade de tratamento de dados pessoais;
- Multas diárias, ou multa simples de até 2% do faturamento, até o limite de 50 milhões de reais.

É importante ressaltar que o controlador e o operador poderão responder conjuntamente ou individualmente pelos danos causados aos titulares dos dados pessoais em caso de incidente ou descumprimento da Lei. Também devemos lembrar que **quando ocorrer qualquer tipo de situação que coloque em risco o titular, é preciso que o mesmo seja informado**.

Contudo, além das penalidades previstas na LGPD, é possível que o titular entre com um processo judicial contra a empresa pelo mal-uso dos dados, por exemplo, ou a empresa pode até mesmo ter sua reputação denegrida diante de seus clientes e de todo o mercado por conta de um incidente de segurança sofrido e amplamente divulgado.

7 Direito dos titulares

A LGPD visa proteger os direitos fundamentais de privacidade, autodeterminação informativa, liberdade de expressão, informação comunicação e opinião, assim como a dignidade e o exercício da cidadania dos indivíduos.

Os direitos dos titulares não podem ser negados em momento algum, devendo ser fornecidos de forma simples, gratuita e de fácil acesso pelo titular. A lei prevê que o titular tem direito de obter do controlador, que realize o tratamento de seus dados (do titular), a qualquer momento e mediante requisição:

Confirmação
confirmar se o controlador possui dados daquela pessoa.

Acesso
solicitar acesso aos dados tratados.

Retificação
atualizar, corrigir ou completar algum dado.

Cancelamento
revogar o consentimento.

Oposição
opor ao tratamento feito pela empresa.

Portabilidade
transferência de dados de uma empresa para outra.

Compartilhamento
questionar sobre quais são as entidades públicas e privadas com quem os dados foram compartilhados.

Revisão das decisões
rever decisões automatizadas realizadas por sistemas oi inteligências artificiais.

8 LGPD X LAI

A Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD) são legislações complementares. A LAI garante o acesso dos cidadãos à informação e a LGPD garante a privacidade dos dados dos cidadãos.

Enquanto a LAI é aplicada em forma de mandato nos entes da administração direta e indireta nos três poderes quando da produção de informação de interesse público, a LGPD é aplicada também na esfera privada, garantindo a proteção dos indivíduos em todos âmbitos por meio da imposição de requisitos àqueles que tratam os dados, como mapeamento das informações utilizadas, posse de um arcabouço de documentos relativos à privacidade e proteção de dados, além da nomeação de um Encarregado de Dados para fazer a intermediação entre a empresa, os titulares e a ANPD.

Ambas as leis buscam resguardar a informação pessoal de terceiros não autorizados, porém apenas a LGPD decanta na preocupação em documentar a análise de impacto à proteção de dados pessoais, a política de privacidade e proteção de dados e a política de respostas a incidentes.

9 LGPD X Serviço Público

O tratamento de dados pessoais pelas pessoas jurídicas de direito 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.

Consideram-se pessoas jurídicas de direito público para fins da LGPD: os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais.

10 LGPD aplicada às empresas de Agronomia

Como já mencionado, as obrigações colocadas pela LGPD são atreladas a quaisquer situações que envolvam dados relacionados a pessoas naturais identificadas ou identificáveis.

Empresas e profissionais que atuam no setor agronômico, lidam, diariamente, com uma grande variedade de dados, tais como, dados pessoais de produtores rurais, clientes, fornecedores, parceiros, colaboradores, e dados de negócio como, volume de produção, geolocalização e/ou georreferenciamento, dados sobre colheita e resultados financeiros e muitos outros que podem vir a identificar uma pessoa natural.

Normalmente as empresas atuantes desse setor utilizam diversas soluções de inteligência artificial no desempenho de suas atividades, como técnicas modernas de mapeamento climático, de produtividade, geolocalização entre outros processos tecnológicos que se utilizam de grandes bases de dados composta por dados pessoais e não pessoais.

Desse modo, percebe-se que a todo instante, dados pessoais são tratados nas atividades agronômicas, sendo inerentes ao negócio e, portanto,

a LGPD não é uma opção, mas uma realidade do setor

devendo os agentes que realizam o tratamento desses dados pessoais implementarem medidas técnicas, jurídicas e organizacionais, a fim de eliminar e minimizar os riscos e problemas resultantes da atuação em desconformidade com a lei.

Recomenda-se, assim, a implementação de um programa de governança em privacidade que estabeleça uma infraestrutura robusta de proteção de dados nas empresas do setor agronômico, cobrindo políticas e processos que envolvam o tema e que defina papéis e responsabilidades para cada agente dentro da organização.

O programa de privacidade ajudará a organização a demonstrar transparência e responsabilidade na proteção dos dados pessoais, gerando confiança nos titulares de dados e parceiros de negócio, além de proteger a reputação em um mundo onde a proteção de dados tem um papel cada vez mais sensível e relevante.

11 LGPD APLICADA ÀS ASSOCIAÇÕES FILIADAS AO IPEEA

No caso das associações, percebe-se naturalmente que diversas operações de tratamento de dados pessoais são realizadas, como:

coleta de dados para cadastramento do associado, inscrição em palestras e cursos, preenchimento de formulário de contato; obtenção de dados financeiros referente ao pagamento das anuidades; dados de colaboradores; retenção de currículos para envio às empresas parceiras; dados de quem navega no site da entidade, como dispzzositivo utilizado, endereço IP, termos de busca, cookies, entre outros.

compartilhamento dos dados com empresas provedoras de benefícios aos associados, como: empresas de lazer, saúde e bem-estar, equipamentos, escolas de idiomas, entre outros;

disponibilização de informações pessoais dos associados no site da associação, como: nome, endereço, data de aniversário e foto;

É evidente que as associações utilizam uma enorme gama de dados pessoais, sendo fundamental saber como este tratamento deve ser feito, garantindo a privacidade dos usuários e fazendo a gestão adequada dos dados.

O tratamento em desconformidade com a legislação, poderá gerar a aplicação de multas, indenizações e diversas outras sanções.

Desse modo, **apesar do seu caráter sem fins lucrativos, a devida adequação das associações à LGPD mostra-se imprescindível**, e a completa implementação de um programa de conformidade é medida que se impõe para evitar os prejuízos nessa seara.

Confira algumas recomendações importantes a serem observadas pelas associações para uma maior conformidade à LGPD:

- Na coleta de dados pessoais, **certifique-se de que está coletando apenas os dados considerados necessários** para a finalidade indicada;

- Nas relações com terceiros, **faça a gestão dos fornecedores**, estabeleça relações comerciais somente com aqueles que adotem boas práticas relativas à proteção de dados, pois em casos de incidentes com esses terceiros, a associação poderá ser responsabilizada;

- Insira **cláusulas de proteção de dados pessoais** nos contratos;

- **Conscientize os colaboradores** quanto à importância e aplicação da LGPD e realize treinamentos;

- Crie **Políticas de Privacidade que estabeleçam diretrizes claras** sobre todo o ciclo de vida dos dados pessoais: como são coletados, para quais finalidades são tratados, com quem serão compartilhados, forma de contato, entre outros;

12. LGPD aplicada às Empresas de Engenharia

Neste tópico, iremos discorrer sobre os principais pontos de adequação à LGPD aplicados às empresas de engenharia, considerando as particularidades do setor e os desafios encontrados para a conformidade com a lei.

Para tanto, os pontos tratados são:

- Mapeamento de dados
- Relacionamento com os titulares
- Coleta de dados
- Arquivamento e eliminação
- Processo de venda
- Dados de colaboradores
- Compartilhamento de dados
- Documentos e Contratos
- Contratos com terceiros
- Segurança da informação

Mapeamento de dados:

A logística do mercado de engenharias traz desafios específicos quando se trata de LGPD, para que essas empresas estejam adequadas às normas de proteção de dados pessoais é necessário o conhecimento dos dados que serão tratados e seus respectivos fluxos.

O mapeamento de dados é um ponto fundamental no processo de adequação e, a partir dele, se é possível definir qual o melhor caminho para a adequação à lei, trazendo à organização maior clareza e entendimento na gestão dos dados.

Coleta de Dados:

Um dos principais pontos de atenção é justamente como se dá a coleta de dados de potenciais clientes ou leads.

Essa coleta poderá ser realizada de diferentes formas:

- **Campanhas de e-mail marketing;**
- **Contato por e-mail por parte do titular;**
- **Chats e formulários no site;**
- **Dados coletados por parceiros;**
- **Dados coletados em estantes de vendas;**
- **Dados coletados ou compartilhados em obras, dentre outros.**

É necessário observar os princípios da LGPD para que se tenha uma coleta de dados adequada.

Segue um checklist com algumas indicações para a coleta adequada de dados:

- [x] Defina uma finalidade clara para a coleta de dados
- [x] Analise se os dados coletados são realmente necessários para atender a finalidade informada;
- [x] Certifique-se que o titular de dados tem informações claras a respeito de como seus dados serão utilizados;
- [x] Descreva em avisos e políticas de privacidade todo o ciclo de vida do dado pessoal;
- [x] Realize treinamento sobre a LGPD com todos os colaboradores que participam do processo de tratamento de dados;
- [x] Defina uma base legal para tratamento de dados;

Cuidado! O consentimento não é a base legal mais adequada na maioria das vezes e caso seja necessária, ele deve ser obtido de forma livre, informada e inequívoca, com a adoção de mecanismos de preservação da obtenção desse consentimento.

Processo de Venda:

Identifica-se no processo de venda, uma série de riscos em termos de LGPD, pois o seu fluxo perpassa pelo processamento de diversas informações, como: levantamento de dados de clientes, fornecedores, colaboradores, dados financeiros, compartilhamento de dados com outros atores, entre outros fatores, sendo de suma importância que esse processo esteja em consonância com as normas de proteção de dados pessoais.

Segue um checklist com recomendações a serem aplicadas nos processos de venda:

- Adote um protocolo específico e bem delineado de como o processo de venda é realizado, com a determinação de fluxo a ser seguido por todos os envolvidos, com critério para a coleta, o acesso e o compartilhamento de dados.
- Obtenha de todos os envolvidos no processo de compartilhamento a assinatura de termos de confidencialidade, bem como realize treinamento em LGPD com eles;

- Crie espaços seguros para o armazenamento de dados;
- Estabeleça critérios e limites para que não haja cópias excessivas ou indevidas dos dados;
- Estabeleça controles de acesso, permitindo que apenas as pessoas que de fato precisam tenham acesso aos dados pessoais;
- Defina regras de compartilhamento de dados, evitando o compartilhamento em plataformas inseguras;
- Verifique se os dados coletados para o processo de venda são necessários à sua finalidade;
- Certifique-se de que o titular seja informado com clareza a respeito da utilização dos seus dados

Compartilhamento de Dados

É comum nas atividades das empresas do ramo de engenharia o compartilhamento de dados com diversos atores, como por exemplo: entre construtoras e imobiliárias, empresas de software, escritórios de advocacia, empresas de marketing, instituições financeiras, parceiros de negócios, investidores, entre outros.

Por ser um uma atividade de tratamento de dados, o seu compartilhamento precisa ser adequado às normas da LGPD.

Para tanto, segue um checklist com recomendações para a realização adequada do compartilhamento de dados:

- [x] Certifique-se da real finalidade e necessidade do compartilhamento, minimizando o volume de dados repassados;
- [x] Oculte as informações que são desnecessárias para a atividade do terceiro;
- [x] Verifique previamente que o terceiro que receba dados tenha preocupação equivalente com o tema e possa garantir segurança adequada.
- [x] Delimite a finalidade de atuação do terceiro, para que não seja extrapolada;
- [x] Deixe claro para o titular, de forma facilitada, as informações sobre o compartilhamento de dados. Lembre-se que ele tem, por lei, o direito de saber com quem seus dados são compartilhados.
- [x] Instrua todo os envolvidos no compartilhamento a respeito das regras para garantir a proteção dos dados (como, por exemplo, restringir o compartilhamento por aplicativos como WhatsApp e excluir os dados armazenados em dispositivos móveis).

Contratos com Terceiros

Como vimos no item sobre compartilhamento de dados, o envolvimento de terceiros é extremamente comum. Além dos cuidados específicos no compartilhamento de dados com esses parceiros, é preciso levar em conta também os cuidados na hora de escolhê-los.

Isso porque todos os envolvidos no tratamento de dados (ou seja, na sua coleta, uso, compartilhamento etc.) respondem solidariamente em caso de danos causados por violações à LGPD.

Desse modo, uma violação cometida por uma das partes afeta diretamente a outra.

Assim, as empresas precisam escolher bem os parceiros com os quais irão estabelecer relações comerciais, a seguir, apresenta-se um checklist a ser observado nessa relação com terceiros:

- Mapeie e avalie todos os contratos já existentes;
- Classifique os contratos considerando o grau de risco em relação ao compartilhamento de dados, destacando os que precisam de atenção redobrada ou alterações urgentes.
- Analise o grau de maturidade e aderência do terceiro à LGPD.
- Estabeleça cláusulas e regras especificas para a LGPD, prevendo, inclusive, a possibilidade de auditorias para avaliar a situação do parceiro em relação ao tema.
- Priorize a segurança da informação, questionando o potencial parceiro a respeito das medidas que a empresa adota.

Relacionamento com os titulares:

A LGPD surgiu para regular o tratamento de dados pessoais, protegendo o titular e dando a ele mais controle dos seus dados. Assim, pode-se dizer que o titular é o ponto focal da lei, a razão pela qual ela existe.

Para as empresas que querem garantir uma boa prática de privacidade e proteção de dados, o relacionamento com o titular deve ser ponto prioritário.

Checklist para um relacionamento adequado com os titulares de dados pessoais:

- Estabeleça uma comunicação clara com o titular, deixando-o informado a respeito do que é feito com os seus dados – especialmente sobre com quem eles são compartilhados (financeiras, bancos, corretores etc.).
- Lembre-se que o titular deve estar ciente da finalidade do tratamento, entendendo quais dados são tratados e por quê.
- Tenha um canal de comunicação acessível, como um e-mail próprio ou um formulário de contato no site, para que o titular possa requerer informações e solicitar o cumprimento dos seus direitos.
- Crie um protocolo de respostas às solicitações do titular para tornar fácil e ágil o seu atendimento. As empresas precisam estar preparadas para receber, analisar, atender e até mesmo negar as requisições do titular, se for o caso.
- Treine funcionários, colaboradores e parceiros para que conheçam os direitos dos titulares e saibam responder os principais questionamentos que possam surgir.

Arquivamento e Eliminação de Dados

O tratamento de dados não termina apenas com a coleta do dado e o seu uso para uma finalidade específica. O arquivamento e a posterior eliminação dos dados também são consideradas atividades de tratamento e, portanto, estão sob o escopo da LGPD.

A LGPD prevê que haverá o término do tratamento quando:

- **Verificada que a finalidade foi alcançada**
- **Quando os dados deixaram de ser necessários à finalidade almejada;**
- **Com o fim do período de tratamento;**
- **Quando houver comunicação do titular;**
- **Por determinação da ANPD.**

Checklist para uma adequada realização do arquivamento e eliminação de dados:

- [x] Crie um protocolo para determinar por quanto tempo cada dado pessoal será mantido.
- [x] Certifique-se de que os parceiros comerciais que também precisam armazenar dados dos seus clientes estão aderentes à LGPD e adotam medidas de segurança adequadas.
- [x] Promova o direito do titular de dados em de requerer à eliminação de seus dados.
- [x] Armazene os dados de forma segura, em formato físico ou digital, com controle de acesso. Apenas quem realmente precisa dos dados para trabalhar deve ter acesso a eles.
- [x] Invista em medidas de segurança para proteger os dados contra cópia, roubo, perda ou destruição.
- [x] Crie e teste um plano de backup e recuperação de desastres.
- [x] Garanta a eliminação segura dos dados quando for a hora, preservando o sigilo das informações.

Dados de Colaboradores:

Quando falamos em LGPD, é comum pensarmos imediatamente na proteção de dados de clientes. Porém, é fundamental lembrar que os funcionários também são titulares de dados e estão protegidos sob a LGPD, nesse sentido, é preciso cuidar dos dados dos seus colaboradores com o mesmo cuidado dispensado aos dados de clientes.

Checklist para uma adequada gestão de dados de colaboradores:

- Reflita sobre quais informações realmente são necessárias para as entrevistas de seleção e recrutamento, evitando a coleta excessiva de dados;
- Evite a coleta de dados pessoais sensíveis, como os relacionados à orientação sexual, etnia, saúde, religião, política etc.
- Adote medidas de segurança tão reforçadas quanto as que são adotadas para os dados de clientes.
- Inclua avisos de privacidade específicos nos formulários, anúncios de vagas e contratos de trabalhos;
- Arquive os dados dos colaboradores pelo tempo previsto em lei, excluindo-os ao fim do prazo.
- Da mesma forma que com os dados de cliente, adote um protocolo para responder às requisições de colaboradores e ex-colaboradores a respeito de seus dados pessoais.

Documentos e Contratos:

Todo programa de adequação à LGPD deve prever a elaboração de documentos e políticas, assim como a revisão e criação de contratos e cláusulas.

Cada empresa possui uma necessidade diferente, que deve ser avaliada pela equipe responsável pelo projeto de conformidade.

No entanto, há alguns documentos que, de maneira geral, são imprescindíveis. No checklist a seguir separamos os mais importantes:

- [x] Avisos de privacidade voltados ao público externo;
- [x] Avisos e política de privacidade para colaboradores;
- [x] Política de retenção de dados;
- [x] Cronograma de retenção de dados;
- [x] Quando aplicável, formulário de consentimento do titular;
- [x] Contrato de processamento de dados com parceiros;
- [x] Quando aplicável, relatório de impacto à privacidade;
- [x] Modelo de resposta e notificação de violação de dados
- [x] Registro de violação de dados
- [x] Formulários e notificação à ANPD
- [x] Cláusulas contratuais com parceiros quanto à necessidade de Compliance.

Segurança da informação:

Não existe privacidade sem Segurança da Informação.

Entender as vulnerabilidades da organização e consertar referidas falhas de segurança, para impedir invasões, vazamentos, entre outros, deve ser prioridade na implantação de qualquer programa de conformidade.

Mais do que boa prática, a segurança da informação é uma obrigação legal. O artigo 46 da LGPD impõe aos agentes de tratamento a adoção de medidas de segurança dos dados pessoais, tornando-a um requisito de conformidade.

Checklist para Segurança da Informação:

- [x] Treine colaboradores e estabeleça políticas claras de segurança;
- [x] Crie mecanismos de autenticação e controle de acesso, restringindo quem pode acessar dados pessoais;
- [x] Desenvolva um plano de backup e recuperação de desastres, seguindo a regra 3-2-1: ter ao menos 3 cópias dos dados, armazenadas em 2 mídias diferentes e com 1 cópia fora do ambiente local.
- [x] Faça um inventário e mapeie os dispositivos de hardware e software utilizados na rede.
- [x] Invista na segurança de endpoints, e-mail, web e redes.
- [x] Avalie a segurança de parceiros e fornecedores;
- [x] Proteja o ambiente de TI e os dados armazenados em meio físico.

13. Como se adequar à LGPD na prática?

Este tópico sugere uma metodologia a ser utilizada em projetos de conformidade à LGPD em empresas de todos os tamanhos, oferecendo uma visão geral do que precisa ser feito e no que consiste cada fase.

Uma das formas mais comuns de conduzir um projeto de conformidade é **a metodologia de 6 fases**, que são:

- Levantamento Inicial
- Plano de Ação
- Data Mapping
- Execução
- Relatório de Risco
- Monitoramento

Por meio desta metodologia, cada fase serve de base e suporte para a fase seguinte, conduzindo o projeto de conformidade de forma fluida e coerente.

Embora a conclusão de cada fase seja pré-requisito para a conclusão da fase posterior, em algumas situações (Como descreveremos abaixo), tarefas de duas fases diferentes podem ser executadas paralelamente, a fim de garantir maior rapidez ao projeto.

Fase 1

Levantamento Inicial e Conscientização:

Na fase de levantamento inicial e conscientização, a equipe responsável pelo projeto de conformidade faz uma avaliação geral da situação do tratamento de dados da organização, além de iniciar o trabalho de conscientização dos colaboradores da empresa a respeito das principais questões de privacidade, segurança e proteção de dados trazidas pela LGPD.

Assim, o levantamento inicial tem como objetivo conhecer melhor o modelo de negócios da empresa e como ele se relaciona com suas atividades de tratamento de dados pessoais.

Nessa fase, deverão ser realizadas as seguintes atividades:

- Preparação da organização e de seus colaboradores para as atividades de adequação à LGPD;
- Planejamento e apresentação de escopo de stakeholders envolvidos;
- Entrevistas para compreensão do modelo de negócios, fluxos de dados, parceiros, fornecedores e legislação específica aplicável;
- Realização de Workshop de Capacitação com público definido pelo cliente;
- Orientação acerca das principais regulações aplicáveis, assim como seus efeitos para a organização;
- Reunião de kick-off com a equipe interna alocada para o projeto de conformidade;
- Definição de principais marcos de entregas e responsáveis;
- Elaboração de cronograma preliminar para o projeto de adequação;

Fase 2

Data Mapping e Avaliações de Risco:

Concluída a conscientização e o levantamento inicial, temos prontas as bases que orientarão o restante do Projeto de Conformidade.

A fase seguinte é o mapeamento de dados ou Data Mapping, sendo provavelmente, a fase mais importante e trabalhosa de todo o processo.

Durante o data mapping, buscam-se levantar e documentar informações detalhadas sobre as atividades de tratamento de dados na empresa, esse levantamento pode ser realizado de diversas formas, envio de questionários, envio de planilha, entrevistas, por exemplo.

Estas informações serão bem mais detalhadas que as coletadas no levantamento inicial e tem finalidade dupla:

1. Oferecer inteligência de negócios que permitirá à organização uma melhor compreensão de seus próprios fluxos, possíveis riscos envolvidos e oportunidades de otimizá-los;

2. Prestação de contas junto à Autoridade Nacional e a parceiros, podendo ser usado para construir o Registro de Operações de Tratamento e cumprir com as obrigações do Artigo 37 da LGPD.

- Avaliar a conformidade do cliente e de seus fornecedores em relação às exigências regulatórias vigentes, inclusive setoriais;
- Identificar os riscos e efeitos do descumprimento dessas exigências;
- Identificar a finalidade de cada atividade de tratamento de dados;
- Produzir um registro de atividades de tratamento de dados na empresa, para fins de transparência e inteligência de negócios;
- Identificar possíveis dados sendo tratados em excesso, ou inadequados à finalidade atribuída;
- Identificar as bases legais mais apropriadas para cada atividade de tratamento de dados;
- Identificar os agentes de tratamento (Controlador/Operador) de cada atividade de tratamento, suas responsabilidades e meios de compartilhamento;
- Mapear ativos de dados (Sistemas, aplicações, bancos de dados, redes internas etc.) onde são armazenados os principais dados e seus responsáveis;

Fase 4
Plano de Ação

A partir da análise de todas as informações levantadas na fase de mapeamento, será desenvolvido e apresentado um relatório compilado contendo descrição de todas as lacunas encontradas e riscos identificados, bem como diversas sugestões de mitigação destes riscos.

O Relatório de Riscos conterá informação detalhada sobre cada risco, incluindo:

- Qual o risco;
- Seu grau de criticidade para a organização;
- Quais são as medidas mitigatórias sugeridas, e informações gerais sobre elas tais quais custo/benefício, trabalho envolvido, e outras;

O objetivo do relatório de risco é prover o máximo de informação possível aos tomadores de decisão da empresa para que possam decidir qual estratégia de adequação adotar, baseados numa abordagem de gestão de riscos.

Fase 3
Relatório de Risco

Nesta fase, com todas as informações providas pelo Relatório de Risco, o comitê de implementação irá elaborar o Plano de Ação que consiste na sistematização, em um cronograma, de todas as medidas mitigatórias dos riscos identificados na etapa anterior.

Para cada risco, é possível que haja diversas medidas mitigatórias sugeridas, dentre as quais os tomadores de decisão da organização deverão escolher quais serão aplicadas.

A compilação de todas as medidas mitigatórias adotadas deverá ser sistematizada em um cronograma elencando:

1) Descrição da Tarefa ou Medida Mitigatória;

2) Prioridade;

3) Responsabilidade;

4) Prazo de início;

5) Prazo de conclusão;

6) Outras informações relevantes.

O Plano de Ação permitirá dividir as responsabilidades, estabelecer prazos e prioridades, e orientar a fase seguinte, de execução.

Fase 5
Implementação

Uma vez consolidado e validado o Plano de Ação, o comitê de implementação pode finalmente pôr as mãos na massa no que diz respeito à execução das medidas mitigatórias discriminadas no Relatório de Riscos e definidas pelo Plano de Ação

Dado que cada organização terá um Relatório de Riscos diferente e, portanto, um Plano de Ação único, é impossível precisar exatamente o que precisará ser feito nesta fase para todas as organizações.

Geralmente, estas ações envolvem:

- Elaboração e inclusão de cláusulas contratuais de proteção de dados em contratos com operadores e fornecedores;
- Elaboração de Políticas diversas: Política de Privacidade, Política de Incidentes, Política de Atendimento aos Direitos do Titular, e outras;
- Elaboração de Relatórios de Impacto à Proteção de Dados;
- Assessoria na revisão de processos de forma a torná-los adequados à LGPD;
- Condução de Testes de Legítimo Interesse;
- Assessoria em Privacy by Design e Privacy by Default para atividades de tratamento incipientes, de forma a torná-las adequadas à LGPD;

A responsabilidade pela execução destas medidas, como já definido no plano de ação, pode ser dos membros do comitê de implementação, de colaboradores da organização, mas também de terceiros contratados para tal, principalmente quando as medidas envolverem a contratação, por exemplo, de softwares e hardware voltados à gestão e garantia da privacidade dos titulares.

Fase 6
Treinamento e Monitoramento

Após a conclusão de todas as tarefas previstas no Plano de Ação, o projeto de conformidade ainda não está completo. Não basta que novas políticas sejam escritas, que contratos sejam revisados e novos processos sejam criados se:

- Os colaboradores da organização não absorveram nem incorporaram ao seu dia-a-dia as mudanças trazidas pelo projeto através de uma capacitação e um treinamento apropriados; e

- As mudanças se revelem incompatíveis com o funcionamento da organização.

A fase 6, portanto, se dedica inteiramente a endereçar estes dois pontos:

1) a capacitação do corpo de colaboradores para seguir o Programa de Privacidade;

2) Sua adequação à realidade da empresa através do monitoramento de seu sucesso e da realização de ajustes pontuais em medidas que não tenham sido bem sucedidas.

O treinamento pode ser realizado com escopo e profundidade variáveis, os colaboradores devem ser treinados às novas regras implantadas, para que todos possam entender e seguir os novos parâmetros estabelecidos em proteção de dados.

Por fim, é importante que o comitê de implementação passe algum tempo monitorando o sucesso das medidas adotadas, coletando métricas para avaliar o sucesso de sua implementação e, quando necessário, fazer alterações necessárias para buscar uma melhor adequação das medidas mitigatórias aos processos da empresa.

O ideal almejado é o de criar uma cultura de privacidade tão arraigada na organização que a observância do Programa de Privacidade se torne tão natural como é a observância a outras questões regulatórias diversas, como as trabalhistas, ambientais, de segurança ou de atendimento ao consumidor.

14. Nomeie um DPO (Encarregado de Dados)

A LGPD, para garantir maior facilidade na gestão dos dados pessoais e assegurar o cumprimento da nova legislação, criou o cargo de "Encarregado", comumente chamado de DPO (Data Protection Officer), que seria o responsável pela regulação do tratamento dos dados pessoais dentro de determinada empresa.

Esse personagem é de extrema importância dentro da LGPD, pois faz com que as empresas se mantenham em dia com as determinações legais, prestando assistência, organizando e determinando a forma de gestão e tratamento dos dados pessoais.

Para conseguir atuar de forma competente e segura, o DPO deverá conhecer e entender por completo todo o fluxo de dados da empresa, de forma que consiga cumprir devidamente com sua função. Portanto, a compreensão de como é feita a coleta, de como e onde os dados são armazenados, quem possui acesso, como se dá o processo de descarte, entre outros, é de enorme importância. Sendo assim, recomenda-se que o DPO passe por treinamentos internos para se adequar ao funcionamento da empresa, e poder compreender perfeitamente todas as ações de tratamento que são realizadas.

Somente assim o DPO poderá iniciar o processo de implementação de uma nova cultura de proteção de dados pessoais. Dessa forma, ele irá começar a cumprir devidamente com suas obrigações de encarregado. Para que a empresa entre em conformidade, serão realizados treinamentos de capacitação dos seus profissionais, visando conscientizar os trabalhadores sobre a nova legislação e sobre práticas que deverão ser observadas daqui em diante.

Ademais, esse encarregado deverá elaborar relatórios de risco, sempre informando e orientando a todos sobre formas de agir para mitigar possíveis danos, como, por exemplo, o incidente ou mal uso dos dados coletados.

Além disso, é papel do encarregado manter uma comunicação direta entre empresa, clientes e a Autoridade Nacional de Proteção de Dados (ANPD), fazendo uma espécie de ponte entre esses elementos, e facilitando, assim, a resolução de eventuais conflitos.

Portanto, pode-se facilmente compreender a necessidade de nomeação de um encarregado capacitado, que consiga cumprir com suas inúmeras tarefas e atribuições.

Se quiser saber mais detalhes sobre quem deve ser nomeado como DPO, suas responsabilidades e penalidades para quem não fizer essa nomeação, clique aqui e baixe nosso e-book sobre o tema.

Baixe nosso e-book!

15. Benefícios de um Programa de Governança

A implementação de um Programa de Governança em Privacidade pode trazer uma série de benefícios e diferenciais para a organização:

- Maior conhecimento e inteligência sobre suas atividades de tratamento de dados;
- Melhor reputação no mercado e no setor;
- Mais oportunidade de negócios;
- Tranquilidade frente às autoridades regulatórias;
- Conformidade às normas de privacidade de forma contínua;
- Ganhos de confiança por parte de titulares dos dados e parceiros de negócio.

Todos esses fatores podem destacar uma empresa em relação as outras, e alavancá-la a um nível de compromisso e seriedade em relação à proteção de dados que é fator comum em todas as organizações de credibilidade internacional.

16. Conclusão

O objetivo desta cartilha é orientar e compartilhar nossa visão e metodologia, de forma condensada, bem como o caminho que entendemos mais eficiente rumo a essa tão relevante conformidade com a LGPD, nos inspiramos nas melhores práticas já utilizadas, visando aplicar uma abordagem simples e condizente com a realidade das organizações na busca pela adequação.

17 □ Sobre o C & V

O escritório Camargo & Vieira é especializado em Proteção de Dados Pessoais e atua em implementação da LGPD em empresas de diversos portes.

Contamos com profissionais que possuem as mais renomadas certificações internacionais, com experiência em diversos segmentos.

Oferecemos uma consultoria de LGPD completa para as empresas de agronomia, engenharia, conselhos e associações de classe, entendemos a complexidade dos setores.

Sabendo portanto da importância e urgência das dos **filiados ao IPEEA** em estarem adequadas à LGPD, nosso escritório oferece de forma exclusiva uma **consultoria gratuita** (de até uma hora) com qualquer filiado ao instituto.

Quer entender mais sobre a LGPD e como ela impacta sua empresa?

Agende uma reunião gratuita.

CAMARGO
& VIEIRA

SOCIEDADE DE ADVOGADOS

camargoevieira.adv.br

relacionamento@camargoevieira.adv.br