CONSCIENTIZAÇÃO

LGPD

O QUE SABER
PARA NÃO FICAR POR FORA!

E-BOOK

Thera
Compliance

Thera Compliance

SOBRE NÓS

A Thera Compliance é uma empresa que procura estar à frente dos principais desafios enfrentados pelas empresas acerca da proteção de dados e segurança da informação.

Formada por um time multidisciplinar de profissionais internacionalmente certificados, a Thera Compliance possui o objetivo de promover soluções de compliance e de propagar uma nova cultura de proteção de dados, de forma holística, ética, responsável e inovadora.

Nos empenhamos a procurar soluções simples e efetivas para os nossos clientes, sempre com o objetivo de minimizar riscos, maximizar lucros e melhorar ainda mais sua reputação perante o mercado.

APENAS UMA NOTA

A LGPD impõe uma profunda transformação no sistema de proteção de dados brasileiro, referindo especificadamente na adoção de medidas de segurança e de boas práticas de tratamento de dados alinhada com a regulação europeia de proteção de dados (GDPR).

É uma lei que estabelece regras detalhadas para a coleta, uso, tratamento e armazenamento de dados pessoais e afetará todos os setores da economia, inclusive as relações entre clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais nacionais e internacionais, além de outras relações nas quais dados pessoais sejam coletados, tanto no ambiente digital quanto fora dele.

Os principais pontos tratados pela LGPD são abordados neste guia de modo objetivo e direto para que o leitor possa ter uma ideia clara sobre os impactos no âmbito empresarial e quais providências deverá tomar para que as medidas necessárias para adequação e compliance sejam adotadas de modo planejado e seguro.

Esperamos que as páginas a seguir sirvam como um "guia de navegação" para essa nova realidade. Lembre- se de que nosso escritório está à sua disposição para que você possa enfrentar, com tranquilidade, esse desafio.

Boa leitura!

*ESTE GUIA NÃO PODE SER USADO COMO OPINIÃO LEGAL E NÃO TEM O OBJETIVO DE ORIENTAR QUALQUER PESSOA PARA FINS LEGAIS.

ÍNDICE

A

Agentes de tratamento:

O controlador e o operador.

Anonimização:

Utilização de meios técnicos que impossibilitam a identificação de quais são e a quem pertence os dados.

Autoridade Nacional de Proteção de Dados (ANPD):

Órgão do Governo responsável por zelar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais.

B

Banco de dados:

Conjunto estruturado de armazenamento de dados, estabelecido em um ou vários locais, em suporte eletrônico ou físico.

C

Controlador

Pessoa ou empresa que é o responsável pelo tratamento de dados por ser a quem necessita ou se beneficia diretamente pelo tratamento.

D

Dados pessoais

Qualquer informação comum que identifique ou possa identificar uma pessoa física, tais como nomes, números, códigos de identificação, endereços.

Dados pessoais sensíveis

É a informação relacionada a uma pessoa natural identificada ou identificável, ou seja, qualquer informação que identifique ou possa identificar uma pessoa, tais como nomes, números, códigos de identificação, endereços.

E

Encarregado de dados ("DPO"):

Pessoa especializada indicada pelo controlador para atuar como canal de comunicação entre ele, os titulares dos dados e a ANPD.

O

Operador:

Pessoa ou empresa que trata os dados a mando do operador

T

Titular dos Dados:

Pessoa física a quem se referem os dados pessoais que são objeto de tratamento, como por exemplo, o cliente, o responsável legal e/ou terceiros (familiares e visitantes).

Tratamento:

Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

O que é?

A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), legislação brasileira que regula as atividades de tratamento de dados pessoais.

Regula o tratamento de dados relacionados a pessoas físicas apenas, excluindo-se, portanto, as pessoas jurídicas.

Aplica-se independentemente do meio e/ou forma de tratamento dos dados; ou seja, impõe regras ao tratamento de dados realizado dentro ou fora da internet, utilizando ou não meios digitais.

Deve ser cumprida por todas as organizações, sejam elas públicas ou privadas, de qualquer tamanho.

Aplica-se a operações de tratamento que ocorrem no território brasileiro, mas também a operações de tratamento que ocorrem fora do país, quando:

- os dados pessoais forem coletados no Brasil;
- os dados sejam relacionados a indivíduos localizados no território brasileiro;
- tiver por objetivo a oferta de produtos e/ou serviços ao público brasileiro.

Não revoga ou impede a aplicação de regulamentos setoriais que tratam sobre proteção a dados pessoais, privacidade e segurança da informação.

Não se aplica ao tratamento de dados pessoais:

- realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- realizado para fins exclusivamente jornalístico e artísticos ou acadêmicos;
- realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais;
- Provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento.

Está valendo desde 18 de setembro de 2020, com possibilidade de aplicação de sanções administrativa a partir de 1º de agosto de 2021.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Artigos 1º, 2º , 3º e 4º.

EM RESUMO, A LGPD VISA PROTEGER DIREITOS FUNDAMENTAIS COMO:

Os dados pessoais são classificados de diferentes formas:

PESSOAIS (COMUNS) - Informação básica relacionada à pessoa natural identificada ou identificável.

DADOS PÚBLICOS - Dados disponibilizados pelo governo e que podem ser encontrados nos sites das autoridades estatais. Seu uso deve respeitar a boa-fé e o interesse público que justificaram sua disponibilização

DADOS MANIFESTAMENTE PÚBLICOS - Dados publicados e compartilhados voluntariamente pelos titulares, como publicações de redes sociais.

QUE PODEM IDENTIFICAR - São dados podem ser entendidos como peças de quebra cabeça, isso porque sozinhos eles não são capazes de mostrar nada, mas se unidos com outros dados pessoais são capazes de identificar um indivíduo. Para exemplificar, "dados identificáveis" podem ser os cookies de um site, nome sem sobrenome, ip de computador, etc.

ANONIMIZADOS - Dados do titular que não podem ser identificados, por estar protegido por tecnologia avançada de proteção de dados.

DADOS SENSÍVEIS - Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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

DE CRIANÇA OU ADOLESCENTE - O Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. A LGPD exige uma proteção especial para essa categoria de dados, determinando que as informações sobre o tratamento desses dados deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação clara e necessária aos pais ou ao responsável legal, bem como adequada ao entendimento da criança.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Artigos 5º, 11 e 14.

Princípios são os valores defendidos e a base de interpretação da LGPD

1. Boa-fé: o uso dos dados deve sempre ter como orientação a honestidade, a intenção de agir de acordo com a lei e o propósito de não prejudicar ninguém.

2. Finalidade: processar para propósitos legítimos (lícitos), específicos, explícitos e informados ao titular.

3. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, conforme contexto.

4. Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

5. Livre acesso: os titulares dos dados devem ter acesso livre, fácil e gratuito sobre a forma e duração do tratamento de seus dados.

6. Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais.

7. Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre o tratamento e os envolvidos.

8. Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

9. Qualidade: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados.

10. Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

11. Responsabilização: agir antes de ser demandado, adotando medidas de cumprimento da LGPD e de prevenção de danos, aptas a demonstrar a conformidade com a lei, caso seja necessário.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Artigo 6º.

Bases legais são as 10 (dez) hipóteses que permitem o tratamento dos dados pessoais:

Mediante consentimento do titular

Para o cumprimento de obrigação legal ou regulatória pelo controlador

Para execução de políticas públicas pela administração pública

Estudos por órgão de pesquisa (sem fim comercial)

Execução de contrato ou de procedimentos contratuais preliminares

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

Para a proteção da vida ou da incolumidade física do titular ou de terceiro

Para a tutela da saúde, por profissionais da saúde ou por entidades sanitárias

Para atender o legítimo interesse do controlador ou de terceiro

Para proteção do crédito

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Artigo 7º.

LEGÍTIMO INTERESSE

Adequado para situações quando:

- **o consentimento do usuário for muito difícil de ser obtido**
- **o consentimento do usuário pode ser considerado desnecessário**
- **houver um impacto mínimo no indivíduo e uma justificativa convincente para a sua utilização**
- **Não afrontar a lei**

CONSENTIMENTO

- **Deve ser por escrito ou por outro meio que demonstre a manifestação de vontade do titular**
- **Pode ser revogado a qualquer momento**
- **Livre informado e inequívoco**
- **Deve ser comprovado pelo Controlador**
- **Estrito à finalidade inicialmente declarada**

O direito dos titulares é o tema mais importante no cumprimento da LGPD

Confirmação da existência do tratamento (em até 15 dias)

Acesso aos dados (em até 15 dias)

Correção de dados incompletos, inexatos ou desatualizados

Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade.

Portabilidade (transferir a guarda) dos dados a outro fornecedor de serviço ou produto

Informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

Eliminação dos dados pessoais tratados com o seu consentimento (há exceções no art. 16).

Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa

Revogação do consentimento

E ainda:

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Arts. 8º, § 5º; 9º, caput; e §3º; art. 14, § 6º e 17 a 22

- §1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
- §2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei
- Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

Uma das partes que requer mais atenção é a hora de dizer "tchau" para os dados que não são mais úteis, porque perderam a finalidade, quando acaba o período de tratamento informado ou porque estão desatualizados.

Dados inúteis ou desatualizados são chamados de "ativos tóxicos" pois representam um constante risco por estarem em desconformidade com a LGPD.

A LGPD estabelece as hipóteses em que os dados devem ser eliminados (art. 15):

- Quando a finalidade for alcançada, ou os dados se tornarem desnecessários ou impertinentes;
- Fim do período de tratamento, quando este for previamente determinado, como no caso de um contrato;
- Se forem coletados com base no consentimento, quando o titular revogar o consentimento;
- Se a Agência Nacional de Proteção de Dados (ANPD) determinar, em caso de descumprimento da LGPD.

Por sua vez, os dados podem ser conservados se (art. 16):

- For necessário para cumprir obrigação legal ou regulatória pelo controlador;
- Forem utilizados para estudo por órgão de pesquisa, garantindo a anonimização sempre que possível;
- For necessário transferir os dados para terceiro, desde que a transferência tenha embasamento legal; e
- Forem mantidos para uso exclusivo do controlador, anonimizados e sem possibilidade de transferência para terceiros.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Artigos 15 e 16.

DIRECIONADAS AOS CONTROLADORES, portanto, em caso de terceirização de serviços, como no caso de contabilidade, é recomendável estipular em contrato a obrigatoriedade de eliminar os documentos em seus prazos corretos, sob pena de alguma sanção.

O não cumprimento da LGPD pode acarretar sanções administrativas, condenações judiciais, irreparáveis danos à reputação da empresa e até perdas de negócios.

ADVERTÊNCIA

com indicação de prazo para adoção de medidas corretivas

MULTAS

Diárias ou simples, de ate 2% do faturamento do último exercício, indo até **50 milhões.**

DANOS À REPUTAÇÃO

Notícias e comentários negativos na internet.

SUSPENSÃO DAS ATIVIDADES

Por até 12 meses.

PROIBIÇÃO DE TRATAR DADOS

Total ou parcial, dependendo da infração.

CONDENAÇÕES JUDICIAIS

Total ou parcial, dependendo da infração.

SANÇÕES ADMINISTRATIVAS

Além da ANPD, outros órgãos, como o Procon, podem aplicar sanções por descumprimentos da lei.

PERDAS DE NEGÓCIOS

Contratar empresas que não cumprem a LGPD é um risco para todos na cadeia de serviços

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Artigos 52 ao 54

A proteção de dados não acontece sem a sua ajuda

Se você é um colaborador, está na linha de frente da segurança da informação e da proteção de dados. É imprescindível que você fique alerta sobre **qual é a sua participação para garantir que os dados sejam protegidos**.

Faz diferença se você trabalha para uma empresa de pequeno ou médio porte?

Empresas menores podem ser ainda mais atraentes para o hackers. Por quê? Geralmente, pequenas e médias empresas possuem uma segurança da informação mais frágil e são mais fáceis de serem infiltradas.

Sua empresa pode ter o melhor software de segurança e as políticas bem elaboradas e abrangentes, no entanto, **suas ações desempenham um papel importantíssimo para ajudar a manter os dados protegidos e evitar incidentes de segurança**.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?

Artigos 46 ao 49

A seguir daremos 9 dicas sobre como você pode ajudar na segurança da informação em sua empresa.

DICAS DE SEGURANÇA DA INFORMAÇÃO

1. Proteja as informações em seu poder

Em sua vida diária, você provavelmente evita compartilhar informações de identificação pessoal, como seu CPF ou número de cartão de crédito, ao responder a um e-mail não solicitado, telefonema, mensagem de texto ou mensagem instantânea. É importante ter o mesmo cuidado no trabalho. Lembre-se de que os cibercriminosos podem criar endereços de e-mail e sites que parecem legítimos. Os golpistas podem falsificar informações de identificação de chamadas. Os hackers podem até assumir contas de mídia social da empresa e enviar mensagens aparentemente legítimas.

Pode parecer óbvio, mas é importante não vazar dados, informações confidenciais ou propriedade intelectual de sua empresa. Por exemplo, se você compartilha uma imagem online que mostra um quadro branco ou tela de computador em segundo plano, pode acidentalmente revelar informações que alguém de fora da empresa não deveria ver.

2. Evite pop-ups, e-mails desconhecidos e links

Cuidado com o phishing!

Phishing é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais, por meio de mensagens eletrônicas falsas.

Os phishers atacam os funcionários na esperança de que eles abram janelas pop-up ou outros links maliciosos que possam conter vírus e malware embutidos. É por isso que é importante ter cuidado com links e anexos em e-mails de remetentes que você não reconhece. Com apenas um clique, você pode permitir que hackers se infiltrem na rede de computadores da sua organização.

Esta é uma regra a ser seguida: **nunca insira informações pessoais ou da empresa em resposta a um e-mail, página pop-up ou qualquer outra forma de comunicação que você não iniciou ou que é inesperada**. Desconfie! O phishing pode levar ao roubo de identidade e também é principal meio para ataques de ransomware (sequestro de informações).

3. Use senhas fortes

Senhas fortes e complexas podem ajudar a impedir que os ladrões cibernéticos acessem as informações da empresa. por sua vez, senhas simples podem facilitar o acesso. Se um cibercriminoso descobrir sua senha, isso poderá dar a ele acesso à rede da empresa, portanto, a criação de senhas exclusivas e complexas é essencial.

Uma senha é forte quando contém pelo menos 10 caracteres, incluindo números, símbolos e letras maiúsculas e minúsculas. As empresas também devem pedir que você altere suas senhas regularmente, por exemplo, a cada 3 meses. Alterar e lembrar todas as suas senhas pode ser um desafio, um gerenciador de senhas pode ajudar.

4. Conecte-se a um Wi-Fi seguro

As redes Wi-Fi utilizadas devem ser seguras, criptografadas e ocultas. Se estiver trabalhando remotamente, você pode ajudar a proteger os dados usando uma rede privada virtual, se sua empresa tiver uma. Uma VPN (Virtual Private Network ou Rede Privada Virtual) é essencial ao trabalhar fora do escritório ou em viagem de negócios. As redes Wi-Fi públicas podem ser arriscadas e tornar seus dados vulneráveis à interceptação.

Mesmo assim, algumas VPNs são mais seguras do que outras. Se sua empresa tiver uma VPN confiável, certifique-se de saber qual é, como se conectar e usá-la.

5. Utilize controles de terceiros

Aqui está um fato que pode ser surpreendente: é comum que as violações de dados comecem dentro das empresas. É por isso que as organizações precisam considerar e limitar o acesso dos funcionários às informações dos titulares.

Você pode ser um encarregado de acessar e usar as informações confidenciais de clientes outros funcionários. Nesse caso, certifique-se de implementar e seguir as regras da empresa sobre como as informações confidenciais são armazenadas e usadas. Se você está encarregado de proteger as cópias impressas ou eletrônicas, você é o defensor desses dados de terceiros não autorizados.

Também é importante restringir o acesso de terceiros a certas áreas, Além disso, lembre-se de desativar o acesso do agente quando o trabalho for terminado.

6. Aposte em sistemas de segurança

Proteções como antivírus forte e detecção de malware, discos rígidos externos que fazem backup de dados e execução de verificações regulares do sistema são investimentos que podem salvar empresas e funcionários de possíveis prejuízos financeiros e jurídicos decorrentes de um incidente de segurança.

Todos os dispositivos que você usa no trabalho e em casa devem ter a proteção de um software forte de segurança. É importante que sua empresa forneça segurança de dados no local de trabalho, mas alerte o responsável pelo TI ou pela Segurança da Informação se encontrar algo suspeito que possa indicar um problema de segurança. Pode haver uma falha no sistema que a empresa precisa ser corrigida e **quanto mais rápido você relatar um problema, melhor.**

7. Instale atualizações de software de segurança e faça backup de seus arquivos

Seguir as práticas recomendadas de segurança de TI significa manter seu software de segurança, navegadores da web e sistemas operacionais atualizados com as proteções mais recentes . As proteções antivírus e antimalware são frequentemente revisadas para direcionar e responder a novas ameaças cibernéticas.

Se sua empresa envia instruções para atualizações de segurança, instale-as imediatamente. Isso também se aplica a dispositivos pessoais que você usa no trabalho. A instalação imediata de atualizações ajuda na defesa contra as ameaças cibernéticas mais recentes.

As ciberameaças geralmente visam seus dados. É por isso que é uma prática recomendada proteger e fazer backup de arquivos em caso de violação de dados ou ataque de malware. Sua empresa provavelmente terá regras sobre como e onde fazer backup dos dados. Arquivos importantes podem ser armazenados offline, em um disco rígido externo, unidade ou na nuvem.

8. Política da Mesa limpa e Tela limpa

A política de mesa limpa e tela limpa se trata de cautelas para assegurar que informações, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets, etc.) não fiquem desprotegidos nos espaços de trabalho e caiam em mãos erradas.

Ao sair de seu posto de trabalho, mesmo que por breve período, é recomendável deixar seu computador bloqueado e protegido por senha **(tela limpa)**, bem como levar consigo seu celular e guardar documentos, papeis, livros ou qualquer outro material que possa conter dados pessoais, que eventualmente estavam sobre a mesa, em alguma gaveta ou arquivo protegido por chave ou senha **(mesa limpa)**.

Outra técnica interessante é a adoção de uma **cultura sem papel**, onde documentos não são impressos desnecessariamente e lembretes não são deixados em monitores ou sob teclados.

Também, todas as informações em quadros brancos deverem ser apagadas e todos os pedaços de papel usados durante uma reunião devem ser descartados apropriadamente após o uso (por exemplo, destruição por picotadora de papel).

9. Siga as orientações e treinamentos

Empresas inteligentes reservam tempo para treinar seus funcionários. Sua responsabilidade inclui conhecer e seguir as políticas de segurança cibernética de sua empresa. Se você não tiver certeza sobre uma política ou procedimento, pergunte!

Quando você usa seu próprio aparelho no trabalho, como um celular ou smartwatch, - Política de Bring you Own Device (BYOD) ou "Traga seu Próprio Aparelho" - pergunte ao responsável pela segurança da informação se o seu dispositivo tem permissão para acessar dados corporativos antes de carregar qualquer coisa nele. Sempre certifique-se de usar aplicativos autorizados para acessar documentos confidenciais.

CONCLUSÃO

A LGPD faz parte de uma mudança de mentalidade mundial, onde os dados deixaram de ser propriedade das empresas e passaram a estar no controle de seus verdadeiros donos: **os titulares**.

Para se manter a proteção de dados é imprescindível manter medidas de segurança da informação, inclusive comportamentais, que se estendem a cada colaborador da empresa, independentemente da hierarquia.

O descumprimento da LGPD não acarreta somente prejuízos financeiros, mas também importantes prejuízos à imagem e perda de negócios.

Em um mundo interconectado, onde todos podem expor suas opiniões na internet, a reputação se tornou um dos mais importantes ativos de qualquer empresa.

Por esse motivo, o cumprimento da LGPD não pode ser pensado somente como o uma medida para evitar punições, mas também como um propulsor do negócio.

MUITO OBRIGADO!

CONTATO

+55 (11) 96919-2375

contato@theracompliance.com

/company/theracompliance

@theracompliance

@theracompliance

www.theracompliance.com