ENTENDENDO A LGPD

UM GUIA PARA EMPRESAS

BROWN PIPE CONSULTORIA

BROWN PIPE CONSULTORIA

Entendendo a LGPD

UM GUIA PARA EMPRESAS

Autores
Guilherme Damasio Goulart
Mariana Ludwig

Editoração e Revisão
Camilla Fanzlau

2024

SUMÁRIO

INTRODUÇÃO

A chegada da Lei Geral de Proteção de Dados Pessoais (LGPD) provocou uma verdadeira revolução no setor de produtos e serviços. A partir de sua entrada em vigor, toda a empresa que trata dados pessoais precisará se preocupar com uma série de disposições técnicas e jurídicas para amparar suas atividades. Trazendo uma série de direitos para os titulares dos dados, a Lei impõe compromissos para as empresas tratarem os dados de forma adequada, importando em uma redefinição das relações entre as empresas e os titulares dos dados.

Por outro lado, suas disposições trazem segurança jurídica para os agentes de tratamento, o que significa dizer que o compromisso com a adequação é uma medida de controle de risco para qualquer organização que não queira arcar com eventuais processos judiciais ou imposições de sanções pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD). São impostas não somente questões procedimentais gerais, mas também de segurança da informação, o que faz com que os agentes de tratamento que realizem a adequação também tenham que observar aspectos tecnológicos de suas atividades.

Assim, este guia apresenta os elementos principais da LGPD, seus pilares fundamentais, em uma visão abrangente, trazendo informações para aqueles que queiram compreender os pressupostos da Lei. Nosso objetivo aqui é proporcionar ao leitor uma compreensão clara e acessível dessa legislação.

02

SOBRE A LEI

SOBRE A LEI

O QUE É A LGPD?

A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2020, é uma legislação brasileira que trata da proteção de dados pessoais de indivíduos (chamados de titulares de dados), ou seja, pessoas naturais. Ela foi inspirada em regulamentações semelhantes, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, e foi criada para estabelecer princípios, regras e diretrizes específicas para o tratamento de dados pessoais no Brasil.

Em resumo, a LGPD tem como objetivo principal proteger a privacidade e os dados de pessoas, garantindo que as organizações que coletam e processam dados o façam de maneira ética, transparente e segura.

03

QUEM É ATINGIDO PELA LEI?

QUEM É ATINGIDO PELA LEI

A LGPD no Brasil atinge vários agentes envolvidos no tratamento de dados pessoais. De acordo com o art. 3º, a Lei cobre as atividades daqueles que realizam qualquer operação de tratamento de dados pessoais, efetuadas por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I. O tratamento de dados seja realizado no Brasil;

II. Os dados tenham sido coletados no território nacional;

III. Ainda que ausente uma das situações anteriormente descritas, o tratamento tem por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no país.

QUEM SÃO AS PESSOAS QUE A LEI ABORDA?

1 PESSOAS NATURAIS (FÍSICAS):

O tratamento pode ser aplicado, por exemplo, se se tratar um influenciador digital, que possui muitos seguidores e está tratando esses dados para fins de publicidade. É possível citar também um médico que atende seus pacientes no seu consultório. Assim, os agentes de tratamento podem ser responsabilizados caso esse tratamento não respeite às determinações legais.

2 PESSOAS JURÍDICAS:

São entidades legalizadas. Podem ser classificadas por direito público (União, Estados, Municípios) e de direito privado (associações, fundações, partidos políticos, entidades religiosas, empresas individuais, bem como as sociedades em geral).

04

QUAIS SÃO AS EXCEÇÕES DA LGPD?

EXCEÇÕES DA LGPD

O art. 4º da LGPD, aponta algumas exceções na aplicabilidade da Lei, o que ocorre nas seguintes hipóteses:

I Realizado por **pessoa natural** para fins exclusivamente particulares e não econômicos. Em resumo, a lei leva em consideração se há qualquer elemento de ganho financeiro ou econômico envolvido na atividade de tratamento de dados pessoais para determinar sua aplicação.

II Para **fins jornalísticos e artísticos.** A exceção se baseia, por meio de uma escolha do legislador, no atendimento dos princípios de liberdade de expressão e comunicação. Isso não significa que tudo seja permitido no campo jornalístico, mas sim que o uso de dados pessoais como fonte de informação não será regulado pela Lei.

III Para **fins acadêmicos**. No caso de análise de diversos tipos de dados pessoais (como históricos, geográficos, biológicos e sociológicos) em que for fundamental para pesquisas acadêmicas. Esta isenção é parcial, já que há ainda a necessidade de se utilizar uma base legal prevista em Lei para o tratamento desses dados.

IV Quando realizado para **fins exclusivos de segurança pública**, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

V Nos casos provenientes de **fora do território nacional** e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

05

DIREITOS DOS TITULARES DE DADOS

DIREITOS DOS TITULARES DE DADOS

A LGPD estabelece diversos direitos para os titulares de dados pessoais. Neste aspecto, destacamos os direitos dos titulares dos art. 9º, 17 e 18 da LGPD.

7 7 7

Ressalta-se que o titular, deve ter um acesso facilitado às informações sobre o tratamento de seus dados. Para atender ao princípio do livre acesso, às informações fornecidas ao titular devem ser disponibilizadas de forma clara, adequada e ostensiva, e devem conter as seguintes características:

- A finalidade específica do tratamento dos dados;
- Por quanto tempo vai durar o tratamento dos dados pessoais;
- Qual é a identificação do controlador dos dados pessoais;
- Informações de contato do controlador;
- Informações acerca se os seus dados pessoais vão ser compartilhados com outra empresa e qual é a finalidade desse compartilhamento;
- Responsabilidade das empresas que realizaram o tratamento dos dados.

7 7 7

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. Ou seja, o artigo estabelece que todas as pessoas **têm o direito** de ser consideradas titulares de seus próprios dados pessoais.

7 7 7

Define os direitos do titular dos dados pessoais em relação ao controlador, definindo diversos direitos que o controlador possui:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

O direito dos titulares dos dados, não aborda apenas as responsabilidades legais que o controlador terá que assumir, mas também as mudanças técnicas essenciais. Essas mudanças técnicas são necessárias para que a pessoa a quem os dados pertencem possa entender completamente quais de seus dados serão usados, por quem e com que finalidade.

06

TRATAMENTO DE DADOS PESSOAIS

DADOS PESSOAIS E SENSÍVEIS

A LGPD garante proteção a todos os dados cujos titulares são pessoas naturais, estejam eles em formato físico ou digital. Assim, a LGPD não alcança os dados titularizados de pessoas jurídicas, os quais não são considerados dados pessoais para os efeitos da Lei. Com isso, define-se dados pessoais e dados pessoais sensíveis da seguinte forma:

1 DADOS PESSOAIS

Conforme o art. 5º, inc. I da Lei, são aqueles dados que permitem a identificação, direta ou indireta, da pessoa à qual o dado se refere (seu titular). Por exemplo: nome, CPF, CNH, carteira de trabalho, data de nascimento, título de eleitor, histórico escolar, e-mail, endereço residencial, dados de compra, transações financeiras, registros de operações em sistemas, etc.

2 DADOS PESSOAIS SENSÍVEIS

Também de acordo com o art. 5º, em seu inc. II, são aqueles relacionados às características mais profundas da personalidade do indivíduo e suas escolhas pessoais. São considerados dados sensíveis: dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dados genéticos ou biométricos.

TRATAMENTO DE DADOS PESSOAIS

O QUE É O TRATAMENTO DE DADOS PESSOAIS?

De acordo com o Art. 5º, inc. X, da LGPD, o tratamento de dados pessoais é toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Nesse contexto, qualquer procedimento que envolva o uso de dados pessoais por meio dessas atividades será classificado como tratamento e estará sujeito às regulamentações estabelecidas pela LGPD.

QUEM SÃO OS AGENTES DE TRATAMENTO?

Os agentes de tratamento, conforme definido pelo art. 5º, IX da LGPD, são as figuras do controlador e do operador de dados pessoais, os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado. São eles que realizam as atividades de tratamento dos dados pessoais de indivíduos (os titulares). Eles têm diferentes responsabilidades no tratamento de dados pessoais dos usuários.

1 CONTROLADOR:

É o agente responsável por tomar as decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento, incluindo as instruções fornecidas para operadores contratados para a realização de um determinado tratamento de dados pessoais. A definição legal de dados pessoais está definida no art. 5º, VI, da LGPD. Muito embora o controlador também trate dados pessoais, o elemento distintivo é o poder de decisão, admitindo-se que o controlador forneça instruções para que um terceiro ("operador") realize o tratamento em seu nome (art. 5º, VII; art. 39 da LGPD). A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um controlador.

- **Controlador Singular:**

É um controlador que opera de forma individual, ou seja, uma pessoa física ou jurídica que

que exerce controle sobre o tratamento de dados pessoais de forma independente e sem compartilhamento de responsabilidades. Isso significa que, neste contexto, um único controlador é responsável por todas as decisões e operações de tratamento de dados.

- **Controlador Conjunto:**

Quando dois ou mais responsáveis pelo tratamento determinam conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento.

2 OPERADOR

A principal diferença entre o controlador e o operador reside no poder de decisão: o operador tem sua atuação limitada às finalidades estipuladas pelo controlador. De acordo com o artigo 5º da LGPD, o operador é definido como pessoa física ou jurídica, tanto de direito público quanto privado, que conduz o tratamento de dados pessoais em nome do controlador. Por outro lado, o artigo 39 da LGPD estipula que o operador deve deve conduzir o tratamento de acordo com as diretrizes fornecidas pelo controlador, sendo este último responsável por assegurar a conformidade tanto com suas próprias diretrizes quanto com quanto com as normas aplicáveis ao assunto. Emerge aqui, portanto, a importância dos contratos de prestação de serviços entre controladores e operadores, eis que a regulamentação das atividades e responsabilidades serão neles definidas.

Os agentes de tratamento devem conhecer os dados que estão sendo tratados, bem como todas as questões técnicas envolvidas. Em geral, tal obrigação é cumprida com a realização e manutenção de inventários de dados pessoais que permitem a organização de todos os dados tratados. Os agentes também devem respeitar os direitos do titular. De maneira geral, os agentes só poderão tratar os dados conforme as disposições da Lei. Assim, além de atender a todos os princípios e hipóteses de tratamento, os agentes devem estar preparados para o atendimento dos direitos do titular. Isso pode envolver, até mesmo, a adequação de sistemas para promover, por exemplo, a possibilidade de apagamento de dados a pedido dos titulares. Tal obrigação abrange ainda um dever qualificado de proteção de dados de crianças e adolescentes.

Igualmente, questões adicionais, como as transferências internacionais de dados pessoais adicionam novas obrigações para os agentes de tratamento.

Embora não seja considerado um agente de tratamento, é importante destacar a figura do **encarregado de proteção** de dados pessoais. Trata-se, segundo a Lei, da "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados", sendo também chamado comumente de Data Protection Office (DPO). Entre suas atribuições, de acordo com o art. 41 da Lei, estão: aceitar reclamações e comunicações de titulares, tomando as devidas providências para atendê-las; receber comunicações da ANPD e atuar para cumpri-las; realizar atividades de orientação, etc. De maneira geral, o encarregado orientará e guiará as atividades de tratamento de dados e adequação por toda a organização. É um cargo de extrema importância e sua atuação é crucial para o sucesso das atividades de adequação à Lei. Por fim, os agentes de tratamento devem sempre indicar um encarregado de proteção de dados, exceto nos casos de agentes de tratamento de pequeno porte, nos termos de resolução já publicada pela ANPD.

07

PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

PRINCÍPIOS DE PROTEÇÃO DE DADOS

No universo do tratamento de dados pessoais, os princípios estabelecidos pela legislação são essenciais. Eles não apenas orientam a licitude e a eticidade nas operações de tratamento de dados, mas também funcionam como um padrão de boas práticas a serem adotadas. A LGPD, em seu artigo 6º, estabelece dez princípios fundamentais para a proteção de dados pessoais. Estes incluem: **finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.**

Esses princípios determinam que todas as atividades de tratamento de dados devem aderir rigorosamente a eles. Por exemplo, ao se analisar os primeiros três princípios - finalidade, adequação e necessidade - percebe-se que é mandatório para os agentes de tratamento avaliar se os dados coletados atendem a um propósito legítimo, específico e claramente informado aos titulares dos dados. Além disso, o tratamento dos dados deve ser proporcional à finalidade, mantendo-se dentro dos limites de adequação e necessidade. Isso significa que a atividade de adequação deve buscar verificar, por exemplo, se para determinada atividade não são recolhidos dados em excesso ou não relacionados com a finalidade daquele tratamento. Um agente que coleta dados pessoais de saúde em uma simples compra de um equipamento eletrônico, por exemplo, provavelmente está descumprindo o princípio da necessidade.

Outro princípio vital é o da **qualidade dos dados**, que assegura que os dados sejam precisos e atualizados. Isso traz para os agentes de tratamento um dever adicional de garantir que não estejam sendo tratados dados incorretos dos titulares.

O princípio do **livre acesso** garante que os titulares dos dados tenham acesso constante e facilitado às suas informações pessoais. Isso significa que os agentes de tratamento devem se preparar (técnica e organizacionalmente) para fornecer os dados do titular de

forma tempestiva. E, sob o escopo da segurança e prevenção, os agentes de tratamento são obrigados a adotar práticas de segurança da informação para prevenir qualquer dano aos titulares dos dados, conforme as disposições da Lei.

Já a **não discriminação** é princípio balizador das relações em que as pessoas possam ser classificadas ou possam ter seu dados tratados com bases em critérios discriminatórios ilícitos. Portanto, classificações desarrazoadas, baseadas unicamente em aspectos discriminatórios que possam prejudicar os seus titulares, são vedadas .Um exemplo dessa violação pode ser o uso de dados relacionados etnia sendo utilizados para desclassificar uma pessoa em um sistema de seleção de candidatos para um emprego.

Esses princípios, portanto, não são apenas diretrizes legais, mas também representam uma base ética fundamental para a gestão responsável e transparente dos dados pessoais.

08

HIPÓTESES OU BASES LEGAIS DE TRATAMENTO

BASES LEGAIS DE TRATAMENTO

As hipóteses legais (ou bases) de tratamento são um requisito a ser observado em toda a atividade de tratamento. O controlador de dados pessoais, ao decidir tratar algum dado, deverá escolher entre as dez hipóteses presentes na Lei a que mais se adeque ao caso concreto. Elas estão definidas no art. 7º da Lei:

I **Mediante o fornecimento de consentimento pelo titular**.
O consentimento do titular ocorre quando o titular autoriza livremente o tratamento das suas informações, desde que tenha sido devidamente informado sobre como serão usados e manifeste claramente a sua concordância. O consentimento é uma das hipóteses mais comuns e ocorre quando o titular diretamente o fornece, em geral marcando opções em sites ou aplicativos ou por meio da assinatura em documentos.

II **Para o cumprimento de obrigação legal ou regulatória pelo controlador.** Muitas leis e normas requerem o tratamento dos dados pessoais de um indivíduo, como para armazenamento de documentos fiscais. Assim, o agente de tratamento, na atividade de adequação, deve verificar quais as legislações ou regulamentos aplicáveis à atividade que obrigam o tratamento de dados pessoais;

III **Pela administração pública**, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

IV **Para a realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;

V **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.
Estes casos envolvem as situações em que o titular está aderindo a um contrato

(de prestação de serviços ou de venda de produtos) ou já possui um contrato em execução e os dados são necessários para permitir a prestação da atividade. A execução do contrato é a base legal para o tratamento de dados pessoais quando essenciais para a realização do contrato com o titular, desde que limitado aos dados necessários.

VI **Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.** O uso de dados em processos judiciais, administrativos ou arbitrais, especialmente para provar algo, é respaldado pela base legal do exercício regular de direitos. É apropriada quando se busca utilizar dados do titular para defender direitos do agente de tratamento em um processo.

VII **Para a proteção da vida ou da incolumidade física do titular ou de terceiro.** Essa situação permite o tratamento e compartilhamento de dados pessoais, quando necessário, para proteger a vida ou a segurança de um indivíduo. Na área da saúde, isso inclui dados como tipo sanguíneo em emergências ou informações do documento de identificação para contatar familiares ou verificar convênios médicos. Legalmente respaldado, o tratamento é válido se visa garantir a vida e a integridade física da pessoa.

VIII **Para a tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. O legítimo interesse do controlador permite o tratamento de diversos dados, desde que não afetem significativamente os direitos dos titulares. Trata-se de uma das hipóteses de tratamento de mais difícil definição e cumprimento, pois impõe obrigações adicionais aos controladores, deixando sua utilização mais complexa.

VI Por fim, para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. É aplicável nos casos em que os dados pessoais são usados para verificar a capacidade de pagamento do titular, como por exemplo, em procedimentos de proteção ao crédito, essa base pode ser utilizada.

09

FISCALIZAÇÃO LGPD

BROWN PIPE CONSULTORIA

FISCALIZAÇÃO

COMO OCORRE A FISCALIZAÇÃO?

A forma de fiscalização padrão ocorre por meio da atuação da **Autoridade Nacional de Proteção de Dados (ANPD).** A ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil. Desta forma, a ANPD atua para assegurar uma ampla e correta observância da aplicação da LGPD no Brasil e, nessa medida, garantir a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos.

QUAL É O PROCEDIMENTO PARA A FISCALIZAÇÃO?

A abordagem da ANDP consiste em priorizar a orientação e a prevenção como primeiras medidas. Contudo, o órgão também tem poder de assumir um papel fiscalizador e de advertência, recorrendo também à possíveis multas nos casos de descumprimento da LGPD, conforme as disposições presentes em suas resoluções. Tudo ocorre por meio de um processo administrativo em que o agente de tratamento tem pleno direito à defesa.

10

PENALIDADES, SANÇÕES E OUTROS RISCOS A EMPRESA

SANÇÕES E OUTROS RISCOS

A LGPD estabelece sanções para os agentes de tratamento que não cumprirem suas disposições. Essas penalidades visam a incentivar a conformidade e garantir a proteção de dados pessoais. Algumas penalidades e outros riscos que as empresas podem enfrentar, de acordo com a LGPD, incluem:

1 SANÇÕES ADMINISTRATIVAS DIFERENTES DA MULTA

Segundo o art. 52 da Lei, podem ser aplicadas as sanções de: advertência, com indicação de prazo para adoção de medidas corretivas; publicização da infração; bloqueio e eliminação de dados pessoais; suspensão parcial do funcionamento de banco de dados; suspensão do exercício da atividade de tratamento de dados pessoais e proibição parcial ou total da atividade de tratamento.

2 MULTAS

A ANPD prevê multas para empresas que violarem a Lei. As multas podem chegar até **2% do faturamento anual** da empresa, **limitadas a 50 milhões** por infração. Isso significa que, em casos graves de não

3 INDENIZAÇÕES:

Além de multas impostas pela ANPD, empresas também podem enfrentar ações judiciais de titulares de dados que alegam danos decorrentes da violação de seus direitos de privacidade, o que pode culminar em indenizações.

4 ATUAÇÃO DE OUTROS ÓRGÃOS

Diante da ligação de muitas atividades de tratamento de dados pessoais com o Direito do Consumidor, o desrespeito à LGPD ainda pode provocar a atuação de órgãos como o Ministério Público e os Procons.

5 COMETIMENTO DE CRIMES

Em casos mais extremos, há até mesmo a possibilidade de cometimento de crimes. Ilustra-se o caso com o crime de "fazer afirmação falsa ou enganosa, ou omitir informação relevante sobre a natureza, característica, qualidade, quantidade, segurança, desempenho, durabilidade, preço ou garantia de produtos ou serviços", conforme o art. 66 do Código de Defesa do Consumidor. Ao menos em tese, aquele agente de tratamento que maliciosa e

intencionalmente engane o consumidor ou omita informações relevantes, quando trata dados pessoais, poderia ser responsabilizado penalmente por sua atuação.

6 REPUTAÇÃO DA EMPRESA

Violar a LGPD pode ter um impacto negativo na reputação e na imagem da empresa. A falta de proteção de dados pessoais dos clientes pode levar à perda de confiança e afastamento dos clientes, bem como problemas contratuais em relação aos parceiros de negócio.

11

SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

É sabido que, atualmente, os criminosos estão cada vez mais especializados no cometimento de novos tipos de fraude. Muitas delas têm como motivação a obtenção de dados pessoais para a realização de outros tipos de fraude e ataques. Tendo isto em conta, e sabendo da importância dos dados pessoais, a **LGPD impôs como princípio e regra a segurança da informação.**

A LGPD é uma das primeiras Leis brasileiras a fixar e delimitar um dever qualificado de segurança da informação. Se até antes de sua entrada em vigor era possível encontrar deveres mais genéricos de segurança, com base no Código de Defesa do Consumidor, por exemplo, agora são estabelecidos deveres mais específicos. No âmbito da segurança da informação, são conhecidos **os atributos de disponibilidade, integridade e confidencialidade**. Portanto, as medidas a serem tomadas pelos agentes de tratamento visam a proteger esses atributos, evitando-se, por exemplo, a violação da confidencialidade, o que pode se dar por meio de um vazamento. O objetivo, portanto, para as empresas, é proteger-se contra situações acidentais ou ilícitas, conforme o art. 46 da Lei, que possam afetar os dados pessoais tratados.

Em qualquer atividade de tratamento de dados pessoais **devem ser tomadas medidas técnicas e administrativas** para proteger os dados tratados. As medidas técnicas são aquelas tomadas por intermédio de meios tecnológicos, como, por exemplo, sistemas aptos a proteger a informação, medidas de autenticação adequadas, medidas para proteger sistemas contra ameaças (como invasões), controle de acesso técnico, realização de backups, criptografia, etc. Já as medidas administrativas envolvem, por exemplo, a criação de políticas, realização de treinamentos, realização de verificações de riscos, etc. Existem normas técnicas específicas no âmbito da Segurança da Informação que indicam melhores práticas a serem adotadas nos ambientes. Uma das mais conhecidas é a ISO/IEC 27002, que elenca diversos controles (alguns considerados técnicos, outros administrativos).

De maneira geral, os agentes devem conhecer os riscos do seu ambiente, o que implica em saber exatamente o contexto em que os dados são tratados, e aplicar medidas para controlar esses riscos.

Às vezes, certas medidas podem ser consideradas tanto como administrativas e técnicas, como a realização de testes de invasão que envolveram análises técnicas em um software, por exemplo, mas que culminarão em recomendações que terão insumos para o controle geral do risco em uma instituição.

De maneira geral, o controlador de dados deve promover todas as medidas técnicas e administrativas, levando em consideração a sensibilidade dos dados e o contexto do tratamento, para evitar incidentes das mais variadas naturezas. Essas medidas devem ser tomadas por todo o ciclo de tratamento de dados. O §2º do art. 46 da LGPD define que as medidas de segurança **"deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".** Define-se, aí, o chamado *privacy by design* e o *security by design*, impondo a verificação de medidas de segurança, inclusive, no início dos projetos que levarão à criação de novas soluções. Esse é um desafio adicional, pois é muito comum que não haja uma cultura empresarial de definição de requisitos de segurança e privacidade logo no início dos projetos.

Outro ponto de relevo se dá acerca do dever de comunicação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares (art. 48 da Lei). Isso significa que os agentes devem estar preparados, em primeiro lugar, para conseguir identificar adequadamente os incidentes ocorridos em seu ambiente. Para tal preparação, medidas administrativas, como uma política de gestão de incidentes, bem como procedimentos para monitorar o ambiente já devem estar em prática, para que o agente, nos casos de incidentes, consiga, em tempo hábil, encaminhar os procedimentos para lidar com a situação. A falta destas medidas, nos casos de incidentes, podem não somente afetar a reputação das empresas, como levar a sanções mais elevadas, quando se verifica negligência ou imperícia na manutenção das medidas de segurança.

12

COMO REALIZAMOS A ADEQUAÇÃO

COMO REALIZAR A ADEQUAÇÃO

Na BrownPipe, entendemos que cada organização possui desafios únicos quando se trata de conformidade com a LGPD. Por isso, nossos serviços buscam oferecer soluções que se adaptam às necessidades das empresas, considerando os recursos disponíveis. São oferecidas três modalidades de serviços, apresentadas a seguir:

1 DIAGNÓSTICO LGPD:

Esta modalidade tem como objetivo realizar uma análise diagnóstica precisa da adequação da sua empresa à LGPD. O processo é desenhado para ser ágil, proporcionando uma visão clara do estado atual de conformidade da empresa. Além disso, delineamos ações prioritárias e necessárias para a completa adequação, destacando os riscos associados e a urgência de certas atividades. De posse do diagnóstico, a empresa pode priorizar e organizar os próximos passos da adequação.

2 ADEQUAÇÃO POR MÓDULOS

Nosso serviço de adequação modular é ideal para empresas que desejam iniciar o processo de conformidade de forma estratégica e gradual. Pensado para atender às necessidades de organizações que preferem começar com ações mais rápidas, específicas e de menor custo, o serviço foca em áreas, processos ou sistemas previamente selecionados, permitindo que sua empresa comece a adequação sem a necessidade de um grande investimento inicial.

Com a adequação modular, você pode abordar as partes mais críticas do seu negócio em primeiro lugar, identificando e corrigindo inconformidades específicas. Isso permite que sua empresa dê os primeiros passos rumo à conformidade de maneira planejada, ao mesmo tempo em que constrói uma base sólida para futuras expansões do processo de adequação.

Como as ações são modulares, o custo efetivo é reduzido, permitindo à empresa conseguir se planejar de forma mais adequada, estabelecendo ações de adequação de acordo com suas possibilidades e prioridades.

COMO REALIZAR A ADEQUAÇÃO

3 ADEQUAÇÃO COMPLETA

AVALIAÇÃO INICIAL (ASSESSMENT)

Nesta etapa, são mapeados os processos de negócio da empresa que tratam dados pessoais, com um foco especial na avaliação dos controles demandados pela lei.

- Mapeamento e Análise: Utilizando a expertise técnica dos consultores da BrownPipe, avaliamos o ambiente por meio do recolhimento de informações técnicas e identificação de gaps e inconformidades com a LGPD.
- Técnicas Avançadas: São utilizadas múltiplas técnicas para esta avaliação, conforme as melhores práticas existentes no mercado, garantindo uma análise profunda e precisa.
- Inventário de Processos: Como resultado, gera-se um inventário de processos, etapa necessária para as atividades de adequação, que permite uma visão clara dos desafios e necessidades.

ADEQUAÇÃO

- Nesta etapa, após concluído o mapeamento dos processos de negócio, são realizadas as atividades de adequação propriamente ditas, que envolvem:
- Apoio na Organização: Auxílio na criação do Comitê Interno Interdisciplinar LGPD (CII) e seleção do Encarregado de Proteção de Dados (DPO).
- Seleção e Priorização: Seleção e priorização dos processos a serem adequados, considerando a importância e o impacto de cada um.
- Implementação do Plano de Ações: Condução e apoio para implementação do plano de ações, garantindo que as medidas tomadas estejam alinhadas com as necessidades identificadas na avaliação inicial.

LÍDERES TÉCNICOS

GUILHERME GOULART

Sócio e Consultor

No âmbito acadêmico é Doutor e Mestre em Direito pela UFRGS. Já ministrou aulas, palestras e seminários sobre Direito da Tecnologia e Segurança da Informação em instituições como Ulbra, Uniritter, UFRGS, UCS, IPA-Metodista, Setrem, FEMA, CGI e também na Escola da Advocacia Geral da União (AGU). Foi professor convidado nos cursos de Especialização em Direito do Consumidor e Direitos Fundamentais e no curso de Especialização em Direito Internacional, ambos da UFRGS. No âmbito internacional, participou como professor das edições IV, V e IV do Curso Luso-Brasileiro em Direito Eletrônico e das Jornadas Luso-Brasileiras do Centro de Investigação de Direito Privado (CIDP), ambos na Faculdade de Direito da Universidade de Lisboa. Foi consultor ad-hoc do Ministério da Justiça em reunião técnica sobre o Debate Público do Anteprojeto de Lei de Proteção de Dados Pessoais em 2015. Foi professor nas pós-graduações do Damásio Educacional, SENAC-RS e Verbo Jurídico ministrando disciplinas. relacionadas com o Direito da Tecnologia, Responsabilidade Civil na Informática e Segurança da Informação. Foi professor na Uniritter na disciplina de "Contratos Eletrônicos" em nível de pós-graduação e no MBA em Negócios Digitais da mesma instituição. É também professor na graduação em Direito das disciplinas Direito das Coisas e Direito das Obrigações no Cesuca.

TEM EXPERIÊNCIA NAS SEGUINTES ATIVIDADES:

- apoio na construção de políticas de TI;
- participação em auditorias de Segurança da Informação (inclusive de acordo com as normas da família 27000);
- apoio na implementação de PKI particular;
- apoio em investigações de incidentes digitais;
- realização de pareceres gerais sobre proteção de dados e segurança da informação;
- análise de risco em atividades de TI e de Segurança da Informação;
- consultoria geral na orientação de atividades relacionadas com Segurança da Informação; e
- apoio na implementação de rotinas de auditoria tecnológica empresarial.

LÍDERES TÉCNICOS

VINÍCIUS SERAFIM

Sócio e Consultor

Mestre em Ciência da Computação pela UFRGS e professor universitário. Atuou como professor em cursos de extensão, graduação e pós-graduação sempre na área da Segurança da Informação e Redes TCP/IP de 1999 a 2023. Já ministrou aulas nas seguintes universidades e faculdades: UFRGS (extensão), UPF, UNISINOS, UCS, ULBRA e Setrem. Atua no mercado como consultor em Segurança da Informação desde 2001, inicialmente por meio da UFRGS/FAURGS e UNISINOS, e, atualmente, com sua própria empresa, tendo acumulado mais de 18 anos de experiência.

7 7

7

- Projeto de pin-pads seguros para bancos;
- investigações de incidentes de segurança (invasão, fraude e mau uso);
- Projetos de sistemas de autenticação;
- Projetos de integração segura de sistemas;
- Projetos de redes seguras;
- Auditorias de segurança;
- Análises de risco;
- Perícias para seguradoras;
- Projetos e implantações de firewalls;
- Testes de intrusão; e
- Projeto de implantação de PKI (ICP).

13

CONTEÚDOS DISPONÍVEIS

CONTEÚDOS DISPONÍVEIS

PODCAST SEGURANÇA LEGAL

2 2

Nós mantemos um podcast que aborda temas envolvendo Segurança da Informação, Proteção de Dados e Direito da Tecnologia. Trata-se do podcast mais ativo no Brasil sobre essa temática. No ar desde 2012, possui mais de 300 episódios. O programa conta com os hosts os sócios da BrownPipe, Guilherme Damasio Goulart e Vinícius da Silveira Serafim.

ALGUNS EPISÓDIOS DESTAQUES SOBRE LGPD:

P _ 1 dSn1 1 1 _ __

S _ 1 dde1 1 1 1 dnnOS

T _ 1 dmp 1 1SO1 _ __ _

U _ 1 dnO1 1 1 1 1 1 _

V _ 1 dnm1 1 1 _ __ 1 _

2 2 2

Além dos conteúdos disponibilizados no Podcast produzimos vídeos no Youtube, abordando temas sobre Segurança da Informação e Proteção de Dados.

2 2

Assista ao vídeo, no qual o sócio e consultor Guilherme Goulart explica de forma clara e objetiva alguns elementos importantes da Lei, como a definição de dados pessoais, o risco de não estar adequado às normas e como podemos ajudá-lo no processo de adequação.

13

SOBRE A BROWNPIPE

BROWN PIPE CONSULTORIA

SOBRE A BROWNPIPE

MISSÃO

A BrownPipe é uma empresa especializada em Segurança da Informação e Proteção de Dados, que tem como objetivo ajudar organizações a proteger seus Dados, Sistemas e pessoas.

VISÃO

Ser reconhecida como referência no âmbito da Segurança da Informação e Proteção de Dados, buscando não somente o crescimento da empresa, mas também o desenvolvimento de nossos funcionários, clientes e da sociedade.

VALORES

ÉTICA, HONESTIDADE, CONHECIMENTO, ESTUDO, EMPATIA, SOLIDARIEDADE

CONTATO

Av. Sen. Alberto Pasqualini, n. 180, sala 2 -
Três de Maio/RS

+(55) 55 2118-1000
www.brownpipe.com.br
www.segurancalegal.com
contato@brownpipe.com.br

NOSSOS SERVIÇOS


Modelagem de ameaças


Análise de Risco e Auditoria


Phishing


Conformidade com LGPD


Políticas de Tecnologia


Compliance


Treinamentos em Palestras


Testes de Invasão


Pentest Contínuo

BROWN PIPE CONSULTORIA

BROWN PIPE
CONSULTORIA

Continuamente protegendo as informações do seu negócio

Entre em contato

Whatsapp: (55) 9916-4209

contato@brownpipe.com.br

www.brownpipe.com.br