



CARTILHA

PROTEÇÃO DE DADOS PARA ASSOCIADOS

ENTENDA O QUE É A

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

ACRJ

A CASA DO EMPRESÁRIO
A CASA DE MAUÁ

PARTE 1 - COMPREENDENDO A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

1.1 HISTÓRICO DA IMPLANTAÇÃO DA LEI

1.2 O QUE É A LGPD?

1.3 O QUE É TRATAMENTO DE DADOS?

1.4 O QUE SÃO DADOS PESSOAIS E DADOS SENSÍVEIS?

1.5 QUEM SÃO OS AGENTES DE TRATAMENTO DE DADOS?

1.6 QUAL A DIFERENÇA ENTRE CONTROLADOR E OPERADOR?

1.7 QUEM SÃO OS TITULARES DE DADOS?

1.8 QUAL O PAPEL DO ENCARREGADO DE DADOS?

PARTE 2 - PRINCIPAIS DIRETRIZES

2.1 O QUE É UM PROGRAMA DE PRIVACIDADE DE DADOS?

2.2 QUAL O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)?

2.3 DIREITOS E DEVERES DOS TITULARES DE DADOS

2.4 DEVERES DO CONTROLADOR

2.5 PAPEL DOS COLABORADORES EM SUA EMPRESA

PARTE 3 - IMPACTOS PARA A EMPRESA PELA NÃO CONFORMIDADE À LGPD

3.1 POSSÍVEIS CONSEQUÊNCIAS

PARTE 4 - BOAS PRÁTICAS

4.1 IMPORTÂNCIA DO DESCARTE DE SEUS DADOS PESSOAIS

4.2 SABIA QUE SEUS DADOS PODEM ESTAR COMPARTILHADOS?

4.3 BOAS PRÁTICAS DE SEGURANÇA EM CELULARES E REDES SOCIAIS

Prezados associados,

A Lei Geral de Proteção de Dados (LGPD), promulgada em 14 de agosto de 2018 e implementada em setembro de 2020, foi concebida com o propósito de normatizar o uso de dados pessoais pelas empresas. Ela estabelece princípios fundamentais de proteção, privacidade, transparência e tratamento adequado dos dados, visando garantir uma gestão responsável das informações pessoais.

A LGPD marca o início de uma nova era de conscientização sobre a privacidade e proteção de dados no país. Isso requer que toda a sociedade compreenda a importância dos dados pessoais e seu impacto nos direitos fundamentais, como a liberdade, a privacidade e o desenvolvimento individual.

A não conformidade com a LGPD pode acarretar danos significativos à reputação de uma empresa. A preocupação dos consumidores com a privacidade e proteção de dados está em constante crescimento. Os prejuízos decorrentes dessa falta de adequação podem ser mais impactantes do que as sanções administrativas eventualmente impostas pela Autoridade Nacional de Proteção de Dados (ANPD).

Nesse contexto, a ACRJ reafirma seu compromisso de auxiliar seus associados na garantia de conformidade em seus processos. Para esse fim, desenvolvemos esta cartilha abordando os principais conceitos e diretrizes da Lei. Além disso, compartilharemos boas práticas de segurança que são relevantes não apenas para as empresas, mas também para todos os seus colaboradores, inclusive como pessoas físicas.

P
A
R
T
E

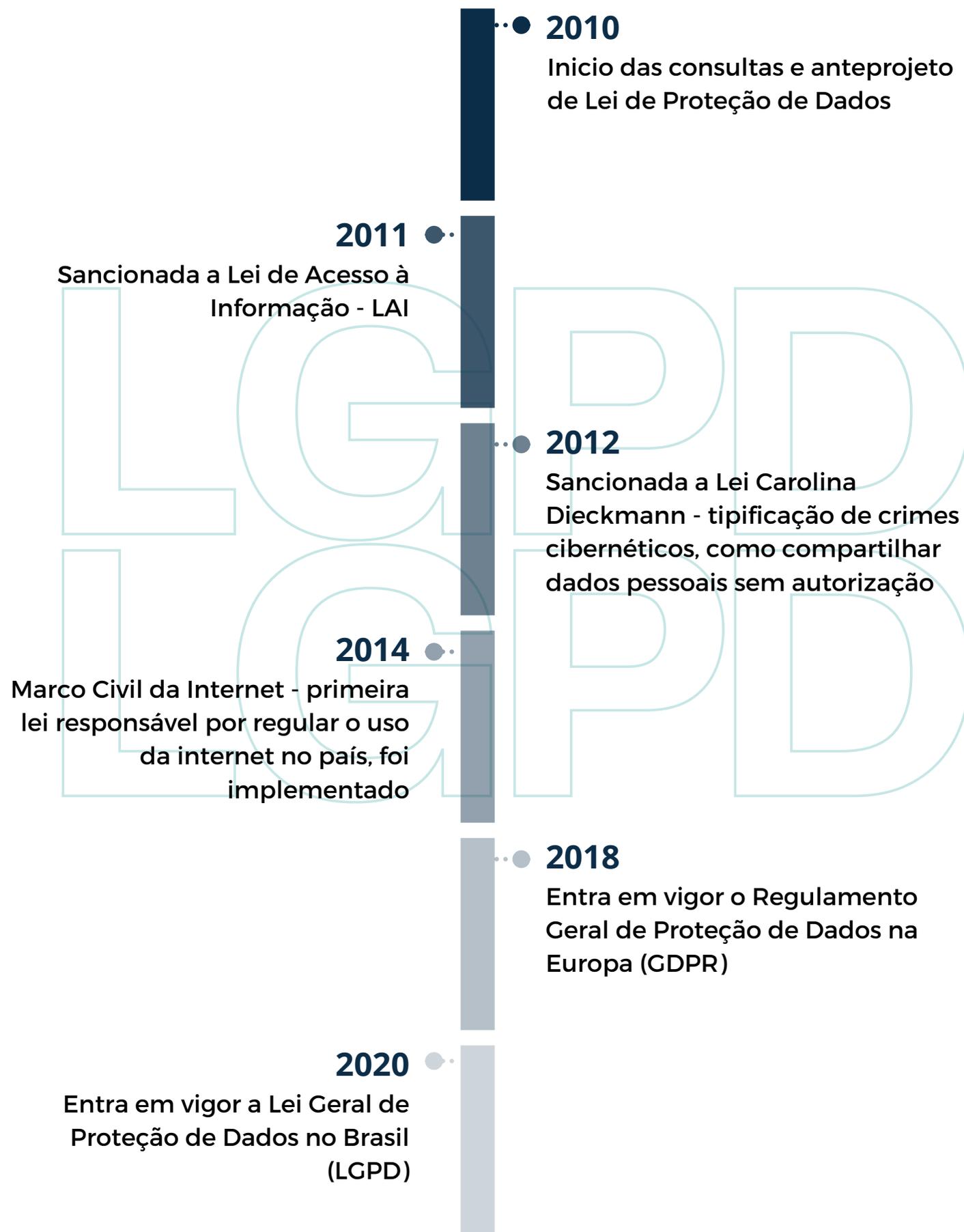
1

COMPREEDENDO A LEI
GERAL DE PROTEÇÃO DE
DADOS

ACRJ

A CASA DO EMPRESÁRIO
A CASA DE MAUÁ

1.1 Histórico de implantação da Lei:



1.2 O que é a Lei Geral de Proteção de Dados?

Como dito em nossa introdução, a LGPD foi concebida com o propósito de normatizar o uso de dados pessoais pelas empresas.

Essa lei tem por objetivo cessar o uso e a comercialização indevida de dados pessoais, inclusive em meios digitais.

As empresas devem respeitar os seguintes princípios na realização do tratamento: se os propósitos são legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

1.3 O que é tratamento de dados?

Considera-se “tratamento de dados” qualquer atividade que utilize um dado pessoal na execução da sua operação, durante o ciclo de vida do dado: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle do dado.

Vale ressaltar que o tratamento de dados requer o consentimento explícito da pessoa para uma finalidade específica. Em algumas situações o consentimento pode não ser obrigatório, dentre outras:

- Cumprir uma obrigação legal;
- Executar políticas públicas;
- Executar contrato com titular dos dados e a pedido desse;
- Prevenir fraudes contra o titular;
- Propiciar a proteção do crédito.

1.4 O que são dados pessoais e dados pessoais sensíveis?

Dado pessoal - informação relacionada a pessoa natural identificada ou identificável, ou seja, qualquer informação que permita identificar, direta ou indiretamente um indivíduo. Exemplos: nome, RG, CPF, gênero, data e local de nascimento, número do telefone, endereço residencial, endereço de e-mail, dados de localização via GPS, placa de automóvel, imagem fotográfica ou computacional, cartão bancário, etc.



Dado pessoal sensível - informação de natureza sensível e privada. Exemplos: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

1.5 Quem são os agentes de tratamento de dados?

São agentes de tratamento o controlador e o operador de dados pessoais. O controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado.

1.6 Qual a diferença entre Controlador e Operador?

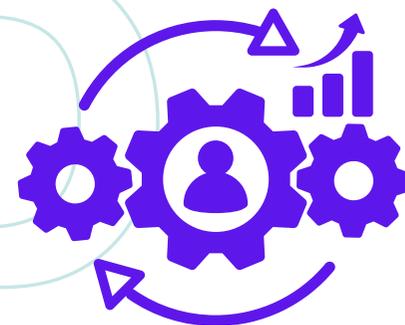


CONTROLADOR - pessoa natural ou jurídica, de direito público ou privado, que:

- Toma todas as decisões referentes ao tratamento de dados pessoais durante o seu ciclo de vida;
- Estabelece os objetivos e os métodos de processamento dos dados pessoais;
- Avalia a adequação das bases legais para o processamento;
- Pode vir a ser responsabilizado por violações da LGPD;
- É responsável por assegurar os direitos dos titulares dos dados.

OPERADOR - pessoa natural ou jurídica, de direito público ou privado, que:

- Executa o processamento de dados em nome do Controlador;
- Não possui poder decisório;
- Pode vir a ser responsabilizado solidariamente por violações da LGPD.



1.7 Quem são os titulares de dados?

O titular de dados é a pessoa física a quem se referem os dados pessoais. É o dono da informação que somente a ele diz respeito.

Pela LGPD toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

1.8 Qual o papel do Encarregado de Dados?



O Encarregado de Dados é o ator responsável por atuar como um canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados – ANPD.

Algumas funções do encarregado de dados:

- Elaborar planos operacionais no processo de implantação de um Programa de Privacidade na empresa;
- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da ANPD e adotar providências;
- Orientar os funcionários e os contratados da empresa a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

P
A
R
T
E

2

PRINCIPAIS
DIRETRIZES

LGPD
LGPD

ACRJ

A CASA DO EMPRESÁRIO
A CASA DE MAUÁ

2.1 O que é um Programa de Privacidade de Dados?

Um programa de privacidade de dados é um instrumento que ajuda as organizações a estabelecer uma infraestrutura de proteção de dados.

Neste instrumento estarão estabelecidas as políticas de gestão e diretrizes de implantação da LGPD na organização. Nele estarão definidas os papéis e responsabilidades de todos os colaboradores da organização.

Neste instrumento também estará descrito todo o processo de monitoramento das atividades relacionados à conformidades e uso dos dados.

2.2 Qual o papel da Autoridade Nacional de Proteção de dados (ANPD)?

A Autoridade Nacional de Proteção de Dados Pessoais - ANPD é uma estrutura 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.

A ANPD está encarregada de elaborar diretrizes para a política nacional de proteção de dados e privacidade, bem como fiscalizar e aplicar sanções em caso de não conformidade com a LGPD. Isso inclui a realização de auditorias e a investigação de práticas de tratamento de dados que possam violar a legislação.

De acordo com a LGPD, cabe ao Encarregado de Dados atuar como canal de comunicação entre o agente de tratamento, ou seja, a organização, os titulares dos dados e a ANPD.

2.2 Direito e Deveres dos Titulares de dados:

De acordo com a LGPD os titulares de dados, possuem alguns direitos e deveres importantes em relação aos seus dados pessoais.

Direitos:

1. **Acesso aos dados:** Os titulares **têm o direito** de acessar seus próprios dados pessoais, podendo solicitar informações sobre quais dados estão sendo coletados, como estão sendo usados e com quem estão sendo compartilhados;
2. **Retificação e atualização:** Os titulares **têm o direito** de corrigir ou atualizar seus dados pessoais caso estejam incorretos, incompletos ou desatualizados;
3. **Portabilidade dos dados:** Os titulares **têm o direito** de solicitar a transferência de seus dados pessoais para outra empresa ou serviço, em um formato estruturado, de uso comum e leitura automatizada, quando isso for tecnicamente possível;
4. **Exclusão dos dados (direito ao esquecimento):** Os titulares **têm o direito** de solicitar a exclusão de seus dados pessoais quando não forem mais necessários para a finalidade para a qual foram coletados, quando o titular retirar seu consentimento ou quando houver uma violação da LGPD;
5. **Revogação do consentimento:** Os titulares **têm o direito** de revogar seu consentimento para o tratamento de seus dados pessoais a qualquer momento, mediante solicitação expressa;

6. Informações claras e transparentes: Os titulares **têm o direito** de receber informações claras, transparentes e acessíveis sobre como seus dados pessoais estão sendo tratados, incluindo a finalidade do tratamento, os tipos de dados coletados, os destinatários dos dados e os direitos do titular.

Deveres:

1. Proteção dos dados sensíveis: Os titulares de dados **têm o dever** de proteger seus próprios dados sensíveis, como informações de saúde, opiniões políticas, religião, orientação sexual, entre outros, e compartilhá-los apenas quando estritamente necessário e com consentimento adequado;

2. Consentimento: Os titulares de dados **têm o dever** de fornecer um consentimento livre, informado e inequívoco para o tratamento de seus dados pessoais, sempre que solicitado pela empresa ou organização que está coletando seus dados.

2.3 Deveres do Controlador:

O controlador de dados tem uma série de responsabilidades sob a LGPD. Aqui estão alguns dos principais deveres do controlador de dados de acordo com a lei:

1. Consentimento: É dever do controlador de dados obter o consentimento expresso e livre dos titulares de dados antes de coletar, usar ou processar seus dados pessoais. Esse consentimento deve ser obtido de forma inequívoca e deve ser revogável a qualquer momento pelo titular dos dados;

2. Transparência e Informação: O controlador de dados tem o dever de fornecer informações claras e transparentes aos titulares de dados sobre como seus dados serão coletados, usados, processados e compartilhados. Isso inclui a divulgação de finalidades específicas para o tratamento dos dados, bem como quaisquer terceiros com quem os dados serão compartilhados;

3. Minimização dos dados: O controlador de dados deve limitar a coleta e o processamento de dados pessoais apenas ao mínimo necessário para atingir as finalidades especificadas. Isso significa que os controladores devem evitar a coleta excessiva de dados que não sejam relevantes para a finalidade do processamento;

4. Segurança dos dados: O controlador de dados é responsável por implementar medidas adequadas de segurança técnica e organizacional para proteger os dados pessoais contra acessos não autorizados, divulgação, alteração ou destruição acidental ou ilícita;

5. Garantia de direitos dos titulares de dados: O controlador de dados deve garantir que os titulares de dados possam exercer seus direitos garantidos pela LGPD, como o direito de acessar, corrigir, atualizar, excluir, portar seus dados, bem como revogar o consentimento quando desejado;

6. Nomeação do Encarregado de Proteção de Dados: É dever do controlador nomear um Encarregado de Dados para atuar como ponto de contato entre a empresa e a ANPD, bem como para garantir o cumprimento das obrigações estabelecidas pela LGPD;

7. Notificação de violações de dados: Em caso de violação de dados pessoais que possa resultar em risco ou dano aos titulares de dados, o controlador de dados tem a obrigação de notificar a ANPD.

2.4 Papel dos colaboradores da empresa:



Os colaboradores das empresas desempenham um papel crucial na implementação eficaz da LGPD em suas organizações. Aqui estão alguns dos principais deveres e responsabilidades dos colaboradores neste contexto.

- 1. Conscientização e Treinamento:** Os colaboradores devem ser devidamente informados sobre as disposições da LGPD e treinados em relação às melhores práticas de proteção de dados;
- 2. Cumprimento das Políticas e Procedimentos:** Os colaboradores devem aderir às políticas e procedimentos estabelecidos pela empresa para garantir o cumprimento da LGPD, ou seja, seguir todas as diretrizes definidas pela empresa;
- 3. Respeito aos Direitos dos Titulares:** Os colaboradores devem respeitar e facilitar o exercício dos direitos dos titulares de dados, como o direito de acesso, retificação, exclusão e portabilidade dos dados. Eles devem responder prontamente as solicitações dos titulares de dados relacionadas aos seus dados pessoais;
- 4. Colaboração com o Encarregado de Dados:** Os colaboradores devem cooperar com o Encarregado de Dados designado pela empresa.

**P
A
R
T
E

3**

**IMPACTOS PARA A
EMPRESA PELA
NÃO CONFORMIDADE
À LGPD**

3.1 Possíveis consequências:

É fundamental que as empresas estejam em conformidade com as disposições da LGPD para evitar impactos negativos. O não cumprimento da LGPD pode resultar em uma série de consequências adversas para uma empresa, citamos as principais consequências negativas:

Danos à reputação: Violações da LGPD podem resultar em danos significativos à reputação da empresa. A perda de confiança dos clientes e fornecedores pode ter um impacto duradouro nos negócios, afetando a imagem da empresa e sua capacidade de atrair e reter clientes;

Perda de clientes e receita: A falta de conformidade com a LGPD pode levar a perda de clientes e a dificuldade em atrair novos clientes. Os titulares de dados estão cada vez mais conscientes sobre a importância da proteção de seus dados pessoais e podem optar por não fazer negócios com empresas que não garantem a segurança e privacidade de seus dados;

Processos judiciais e ações de responsabilidade civil: As empresas que violam a LGPD podem enfrentar processos judiciais por parte dos titulares de dados afetados. Isso pode resultar em ações de responsabilidade civil, resultando em pagamento de indenizações por danos causados aos titulares de dados em decorrência das violações;

Perda de oportunidades de negócios: Empresas que não estão em conformidade com a LGPD podem perder oportunidades de negócios, especialmente em setores onde a conformidade com a privacidade de dados é um requisito contratual ou regulatório. Isso pode limitar a expansão da empresa e sua participação no mercado;

Investigação e ações regulatórias: E por fim, a ANPD tem o poder de investigar e impor sanções administrativas às empresas que descumprem a LGPD.

P
A
R
T
E

4

BOAS PRÁTICAS

LGPD
LGPD

ACRJ

A CASA DO EMPRESÁRIO
A CASA DE MAUÁ

4.1 Importância no descarte de seus dados pessoais:

Os dados estampados em etiquetas e embalagens também são informações pessoais e é importante lembrar de ocultá-las e/ou destruí-las antes de descartar.

Um ponto de atenção são os códigos de barra e QR Codes colados nas caixas e embalagens, eles escondem dados que não conseguimos ver. Os fraudadores podem ler os dados presentes no QR Code e conseguir informações sobre o comprador para usá-los de forma mal-intencionada.

A nossa recomendação é que você rabisque ou destrua todas as etiquetas e embalagens antes do descarte.

4.2 Sabia que seus dados pessoais podem estar compartilhados?

1 Uma prática que se popularizou no Brasil, mas que não é regularizada, é o fornecimento de dados, como o CPF, endereço e até a biometria, durante compras em alguns estabelecimentos. Você já se perguntou com qual finalidade esses dados são coletados?

Os estabelecimentos alegam que a solicitação de dados está vinculada à oferta de descontos. Porém, não é permitido coagir ou forçar o consumidor a informar o CPF para conceder uma promoção.

Esta prática pode levar a um compartilhamento de dados não autorizado, acarretando: vazamento de dados, o uso e compartilhamento indevidos — como a venda não autorizada das informações daquele estabelecimento para outros sem o conhecimento dos titulares dos dados.

A nossa recomendação é que você certifique-se com o estabelecimento a finalidade da solicitação de seus dados pessoais.

2 Está previsto na LGPD que o titular de dados é responsável pela segurança de seus dados pessoais. Com frequência, as pessoas inadvertidamente compartilham seus dados pessoais em suas redes sociais, sem compreender totalmente a amplitude dessa exposição. Seguem algumas formas comuns desse compartilhamento:

- **Postagens públicas:** Muitas pessoas compartilham informações pessoais em suas postagens públicas, como fotos de família, amigos ou eventos, informações sobre seus interesses, hobbies, viagens e até mesmo detalhes sobre sua rotina diária;
- **Check-ins e localização:** Algumas redes sociais permitem que os usuários compartilhem sua localização atual ou façam check-in em locais específicos, o que pode revelar informações sobre onde a pessoa está ou costuma frequentar;
- **Configurações de privacidade inadequadas:** Se as configurações de privacidade de uma conta de rede social não estiverem adequadamente configuradas, as informações pessoais podem estar acessíveis a um público mais amplo do que o desejado, incluindo pessoas que não são amigos ou conexões diretas;
- **Phishing e engenharia social:** Os golpistas podem usar informações pessoais disponíveis em redes sociais para realizar ataques de phishing ou engenharia social, tentando enganar as pessoas para revelar informações confidenciais ou clicar em links maliciosos.

4.3 Boas práticas de segurança em celulares e redes sociais:

Para mitigar problemas como furtos de celulares e invasão de contas, redes sociais e aplicativos de mensageria, seguem algumas dicas:

- 1** Configure o bloqueio de tela e as senhas de acesso a dispositivos eletrônicos;
- 2** Ative a autenticação em dois fatores, especialmente para redes sociais;
- 3** Tenha sempre um backup;
- 4** Configure limites para transações financeiras no Internet Banking e ative a confirmação de compra com senha para dispositivos contactless;
- 5** Use uma marca pessoal em seus cartões para evitar golpes. Pode ser um adesivo, ou algo que você identifique facilmente;
- 6** Tenha contatos de emergência e informações de saúde anotados;
- 7** Instale apps para rastreamento de dispositivos;
- 8** Em caso de furto ou roubo avise a sua família, bancos e operadora de telefonia;
- 9** Evite acessar redes de internet públicas, pode não ser muito seguro.

Avalie a maturidade de sua empresa!

A ACRJ oferece um diagnóstico para identificar o índice de maturidade quanto ao compliance à LGPD. Acesse o QrCode ou clique no link abaixo e responda o formulário.

Questionário LGPD



Ao finalizar o questionário, em até 5 dias úteis, você receberá o resultado por meio de um report executivo que será enviado para o seu e-mail.

ACRJ

A CASA DO EMPRESÁRIO
A CASA DE MAUÁ



[HTTPS://TECHWISE.RIO](https://techwise.rio)



@TECHWISE.RIO



CONTATO@TECHWISE.RIO

CARTILHA PRODUZIDA POR
TECHWISE INTELIGÊNCIA EMPRESARIAL