LEI GERAL DE PROTEÇÃO DE DADOS

Cartilha da Associação Brasileira
de Shopping Centers para seus Associados

ABRASCE

LEI GERAL DE PROTEÇÃO DE DADOS

Cartilha da Associação Brasileira
de Shopping Centers para seus Associados

ABRASCE

ÍNDICE

PALAVRAS DO PRESIDENTE

Caro associado,

Faz parte do compromisso da Abrasce compartilhar conhecimento e instruir nossos associados sobre temas relacionados às operações de um shopping center para desenvolver e fortalecer, cada dia mais, nosso setor.

Neste sentido, estamos lançando uma cartilha com informações sobre a Lei Geral de Proteção de Dados (LGPD), que entrará em vigor a partir de agosto de 2020 e impactará nosso setor de forma significativa, uma vez que estabelece as diretrizes de coleta, armazenamento, compartilhamento e gestão de dados pessoais dos consumidores.

A aprovação de uma lei robusta como a LGPD é um grande marco para o Brasil, que se une ao grupo de países com legislações específicas voltadas para a segurança da informação. Ganham evidência e tornam-se mais fáceis as relações econômicas e comerciais com empresas multinacionais e outros países que também mantêm esse tipo de legislação, o que ainda garante ao Brasil credibilidade e transparência no gerenciamento destas informações.

Daqui para frente, o desafio será grande. São muitos os detalhes, normas e procedimentos aos quais os shopping centers terão que se atentar, além dos investimentos em capacitação, tecnologia e segurança que, em muitos casos, serão inevitáveis.

Espero que, com este material em mãos, o processo de adequação à nova lei seja mais esclarecedor e seguro. Ainda assim, mantemo-nos à disposição para ajudá-lo no que for preciso durante este momento.

Boa leitura!

Glauco Humai
Presidente

1. INTRODUÇÃO

1.1. Contexto

A publicação da Lei Geral de Proteção de Dados (LGPD), em 15 de agosto de 2018, é um importante marco para o mercado brasileiro no tratamento de dados pessoais e faz parte de um movimento mundial de preocupação em relação ao tema e sobre o papel que o Estado deve desempenhar.

Muito da nova lei é inspirado na General Data Protection Regulation (GDPR), da União Europeia, que entrou em vigência em maio de 2018, e que tem como principal foco criar regras de tratamento de dados buscando empoderar o usuário com o controle sobre suas informações. Dessa forma, há um foco grande na liberalidade do usuário em controlar, retificar e excluir seus dados das plataformas.

O novo cenário tem complexidade e os desafios chegam em ritmo acelerado, com foco na adequação de operações e processos trazidos pela nova regulamentação, que passa a vigorar em agosto de 2020. Por isso, a Abrasce, atenta às necessidades de seus associados, coloca seu conhecimento e experiência à disposição para ajudar a tornar o processo mais tranquilo.

1.2. Objetivo

A Lei de Proteção de Dados estabelece os princípios, direitos e deveres que precisarão ser observados, daqui para frente, no tratamento de dados pessoais.

1.3. Abrangência

A LGPD se aplica a qualquer operação de tratamento de dados pessoais (vide definição no item 2), seja por pessoa física ou jurídica, de direito público ou privado, independentemente do meio, país de sua sede ou país onde estejam localizados os dados, desde que:

i. a operação de tratamento seja realizada no Brasil;
ii. a operação de tratamento tenha como objetivo a oferta ou fornecimento de bens, serviços ou tratamento de dados de pessoas físicas localizadas no Brasil;
iii. os dados pessoais tenham sido coletados no Brasil.

Ainda, podem ser considerados dados pessoais, nos termos do §2º do Art. 12 da LGPD, os utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. Por exemplo: cruzamento de bases anonimizadas que levam à identificação do indivíduo.

A LGPD também dá tutela diferenciada e limita as hipóteses de tratamento de dados pessoais sensíveis (Artigo 11) e de crianças e adolescentes (Artigo 14).

1.4. Exceções

A LGPD não abrange o tratamento de dados:

i. por pessoa física, com fins particulares, não econômicos (exemplo: agenda pessoal de contatos; lista de convidados de uma festa particular);
ii. para fins exclusivamente jornalísticos, artísticos e acadêmicos;
iii. para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; atividades de repressão de infrações penais; e
iv. dados provenientes de fora do Brasil e que não sejam objeto de tratamento por agentes de tratamento brasileiros (vide o conceito de "agentes de tratamento" no Capítulo 2).

1.5. Vigência

A LGPD entrará em vigor em agosto de 2020.

2. CONCEITOS

O Artigo 5º da LGPD traz alguns conceitos em seus incisos. Para fins didáticos e facilidade de consulta, foram organizados em ordem alfabética e indicados, entre parênteses, a referência legal.

Agentes de Tratamento: o controlador e o operador (Art. 5º, IX);

Anonimização: meios técnicos por meio dos quais um dado perde a capacidade de identificar uma pessoa física (Art. 5º, XI);

Autoridade Nacional ("ANPD"): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD (Art. 5º, XIX);

Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (Art. 5º, IV);

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (Art. 5º, XIII);

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Art. 5º, XII);

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Art. 5º, VI);

Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável (Art. 5º, I);

Dado Pessoal Sensível: dado pessoal 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, dado genético ou biométrico, quando vinculado a uma pessoa natural (Art. 5º, II);

Dado Anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (Art. 5º, III);

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado (Art. 5º, XIV);

Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (Art. 5º, VIII);

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Art. 5º, VII);

Órgão de Pesquisa: órgão, público ou privado, sem fins lucrativos, com sede e foro no Brasil, que tenha como objeto a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Art. 5º, XVIII);

Relatório de Impacto à Proteção de Dados Pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Art. 5º, VII).

Titular: pessoa física a quem se referem os dados pessoais que são objeto de tratamento (Art. 5º, V);

Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Art. 5º, XV);

Tratamento: 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 (Art. 5º, X);

Uso Compartilhado de Dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (Art. 5º, XVI).

3. PRINCÍPIOS APLICÁVEIS AO TRATAMENTO DE DADOS E DIREITOS DOS TITULARES

Os Agentes de Tratamento devem adotar medidas efetivas para que as operações de Tratamento estejam aderentes aos princípios previstos no Artigo 6º da LGPD:

Princípio da Boa-Fé: princípio geral que permeia todas as relações jurídicas. A boa-fé se presume e a quebra da boa-fé acarreta em consequências jurídicas.

Exemplo: Criar um termo de uso de dados intencionalmente ambíguo para Tratamento de Dados Pessoais para induzir Titular a dar consentimento em mais hipóteses do que gostaria, caso entendesse a redação de forma clara.

Princípio da Finalidade: Os Dados Pessoais devem ser tratados para determinados propósitos, os quais devem ser informados ao Titular dos dados previamente, de modo explícito e sem que seja possível a utilização dos dados posteriormente para outra aplicação.

Exemplo: Dados Pessoais coletados em cupons, no escopo de um sorteio de um prêmio. A cada compra de determinado valor, o consumidor preenche um cupom e o deposita em uma urna do Shopping Center.

O cupom não tem termos de uso e privacidade em seu verso e apenas uma opção para que o consumidor assinale que concorda que, se sorteado, seus Dados Pessoais poderão ser usados para contatá-lo.

O Shopping Center pode armazenar esses dados, criar um banco de cadastro ou usar esses dados para enviar um e-mail marketing ou uma publicidade?

Não, não pode! Qual é a finalidade do tratamento? Identificar e contatar o vencedor do sorteio. Alcançada essa finalidade, os Dados Pessoais devem ser eliminados ou coletados os respectivos Consentimentos para que os mesmos tenham Tratamento distinto da finalidade informada.

Note que o Artigo 7º, § 4º da LGPD, dispõe que os Dados Pessoais disponíveis publicamente não se sujeitam à exigência do Consentimento, mas, pela incidência do princípio da finalidade, não deve ser compreendido como uma "carta branca" para uso irrestrito dessas informações.

Princípio da Adequação: Os Dados Pessoais devem ser usados de modo compatível com a finalidade declarada ao Titular.

Exemplo: O Titular consente o Tratamento de seus Dados Pessoais para recebimento de promoções e cupons de desconto do Shopping Center. O Shopping Center, com base nesse Consentimento, pode compartilhar os Dados Pessoais com uma agência de publicidade para que esta crie uma campanha com base nos Dados Pessoais tratados?

Não, não pode! Para tanto, é necessário solicitar novo Consentimento ao Titular.

Princípio da Necessidade: O Tratamento deve ser limitado ao mínimo necessário para o alcance da finalidade.

Exemplo: Conjugando com o exemplo do Princípio da Finalidade: Dados Pessoais coletados em cupons, no escopo de um sorteio de um prêmio. A cada compra de determinado valor, o consumidor preenche um cupom, e o deposita em uma urna do Shopping Center. Qualquer informação / dado pessoal coletado no cupom que não tenha relação com a identificação e localização do vencedor do sorteio - tais como gênero, orientação sexual, ideologia, filiação partidária ou sindical etc. – não deve ser tratado, já que não é necessário ao conhecimento do vencedor e entrega do prêmio.

Princípio do Livre Acesso: Garantia aos Titulares à consulta facilitada e gratuita sobre a forma e a duração do Tratamento, bem como o acesso à integralidade dos seus Dados Pessoais. Ênfase nos termos “facilitada”, “gratuita” e “acesso à integralidade”.

Princípio da Qualidade: Devem ser garantidas, ao Titular, exatidão, clareza, relevância e atualização dos dados.

Princípio da Transparência: Deve ser garantida a prestação de informações claras e facilmente acessíveis pelos Titulares. O Titular deverá ser capaz de solicitar seus dados, de corrigi-los ou de solicitar sua exclusão de forma rápida, fácil e descomplicada.

Princípio da Segurança: Deverão ser adotadas medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados. O Artigo 46, § 1º e 2º, estipula que, além da responsabilidade pela adoção das medidas de proteção, a LGPD poderá dispor sobre os padrões técnicos mínimos aceitáveis.

Princípio da Prevenção: Deverão ser adotadas medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais. Notem que o princípio é de prevenção. Não bastará mais agir de modo reativo, ou seja, após o acidente. Se uma prevenção não for adequadamente implementada, os pressupostos jurídicos para uma ação de responsabilidade civil estarão postos: houve negligência, ou seja, descumprimento do dever geral de diligência (cuidado) a que todos estamos subordinados. Além do Artigo 46, a lei ainda traz outros elementos no artigo 50 e seguintes, propondo ações de governança e treinamentos.

Princípio da Não Discriminação: Impossibilidade de tratamento para fins discriminatórios. É proibido usar dados para fins que gerem discriminação.

Exemplo: Cadastro em lojas que, com Consentimento, requer a indicação da orientação religiosa e, na época do Natal, apenas concede descontos àqueles que marcaram a opção cristão, não oferecendo o mesmo tratamento aos demais clientes não cristãos.

Princípio da Responsabilização e Prestação de Contas: O Shopping Center deve apontar um Encarregado e atribuir responsabilidades aos seus empregados com a segurança da informação e proteção de dados. A LGPD impõe a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais, que consiste no documento que contém todos os pontos de interesse relativos à proteção de Dados Pessoais, incluindo medidas de segurança e contenção de riscos documentadas, funcionando perfeitamente ao atendimento deste princípio.

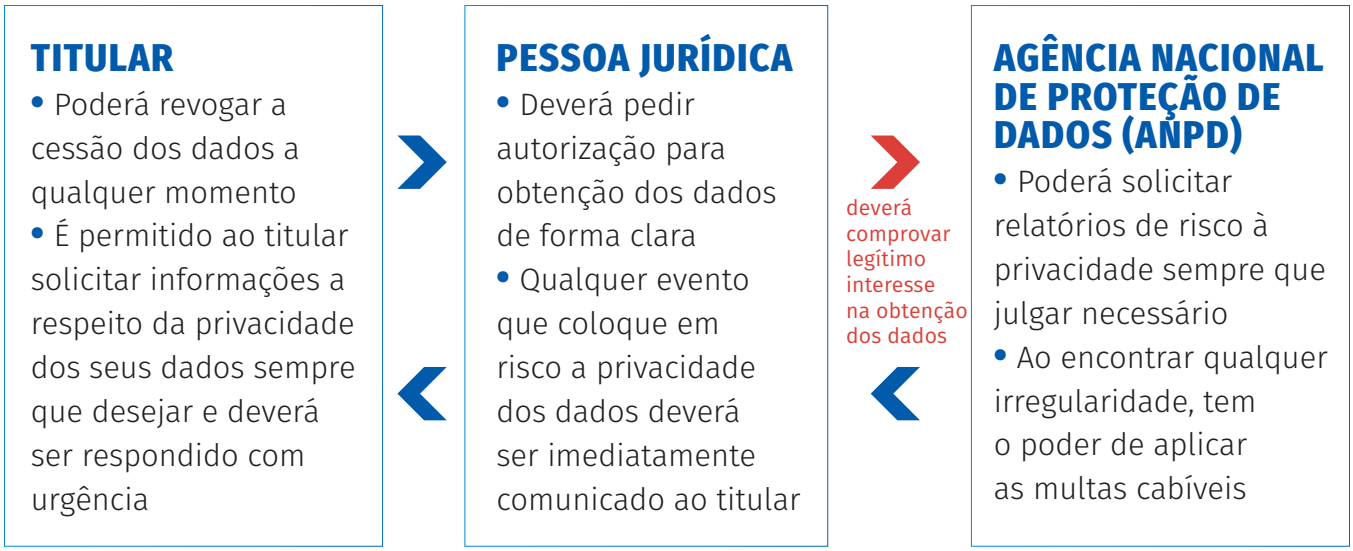
4. HIPÓTESES DE TRATAMENTO DE DADOS

Nos termos da LGPD, o Tratamento de Dados Pessoais somente poderá ser realizado em uma das dez hipóteses previstas nos incisos do Art. 7º. As hipóteses, taxativas, são:

i. mediante o fornecimento de consentimento pelo titular;
ii. para o cumprimento de obrigação legal ou regulatória pelo controlador;
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, observadas as disposições do Capítulo IV desta Lei;
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;
vi. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

vii. para a proteção da vida ou da incolumidade física do titular ou de terceiro;
viii. para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
ix. quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
x. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Nos termos do Artigo 7º, § 4º, é dispensada a exigência do Consentimento para os dados tornados manifestamente públicos pelo Titular, resguardados os direitos do Titular e os princípios previstos na LGPD. Ou seja, os Dados Pessoais podem ser tratados sem o Consentimento, mas balizados pelos princípios e fins legítimos. Não pode ser um Tratamento indiscriminado e abusivo. Não pode apenas atender aos interesses do Shopping Center.



Fonte: https://www.senior.com.br/blog/lgpd-o-que-e-como-vai-funcionar-e-o-que-muda-para-sua-empresa/. Acesso em 12 de jul. 2019.

5. ADEQUAÇÃO AOS TERMOS DA LGPD

5.1. Como se adequar?
Estar adequado à LGPD significa que:

i. os direitos dos titulares de dados pessoais estão assegurados;
ii. o tratamento de dados pessoais respeita os princípios expostos nos incisos do artigo 6º da LGPD e está respaldado por uma (ou mais) das hipóteses previstas nos incisos do artigo 7º da LGPD;
iii. o agente de tratamento, na situação concreta, está ciente de seu papel e adimplente com suas obrigações e responsabilidades;
iv. existe um encarregado de dados indicado; e
v. medidas de segurança e boas práticas foram adotadas e são constantemente revisadas.

5.2. Perguntas a serem respondidas. Passos a serem tomados.
Dados Pessoais já sob Tratamento: Quais Dados Pessoais estão sob Tratamento do Shopping Center? Quais hipóteses legitimam esse Tratamento? Apenas os dados absolutamente necessários para fornecer o serviço estão sob Tratamento?

Direitos dos Titulares: Todos os direitos dos Titulares estão garantidos? O Shopping Center já assegura os direitos dos Titulares? Se não, como irá operacionalizá-los?

Avisos de Privacidade: O Shopping Center tem avisos de privacidade? Em quais situações? Todos são claros e completos e contam com detalhes que permitem ao Titular uma visão ampla de seus direitos e do Tratamento de seus Dados Pessoais?

Fornecedores em Compliance com a LGPD: provedor de serviços de e-mail; serviço de CRM; agências de marketing; relações públicas estão aderentes à LGPD? O Shopping Center pode ser responsabilizado por violações feitas pelos processadores com os quais trabalha. É importante garantir que todos os aspectos do processamento e coleta de dados estejam corretos e respeitando a lei.

Tratamento de Dados, novo procedimento: como são coletados dados hoje? Existe um formulário claro e transparente para Consentimento do Titular? Aviso de cookies? É possível que um Titular alegue dúvidas dos motivos e razões por que os dados estão sendo coletados e para que eles serão utilizados?

6. SANÇÕES E PENALIDADES

A LGPD estabelece penalidades bastante rigorosas (Art. 52):

i. Advertência;
ii. Obrigação de divulgação do incidente;
iii. Eliminação de dados pessoais;
iv. Multa de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos e limitada, no total, a R$ 50 milhões por infração.

As penalidades não substituem a aplicação de sanções administrativas, civis ou penais previstas em legislação específica (art. 52, § 2º) e existem contingências potenciais, tais como: ações individuais de danos morais; rescisão de contratos por quebra de deveres de proteção de dados e sigilo; danos reputacionais; ações promovidas pelo Ministério Público etc.

7. QUESTÕES RELEVANTES PARA SHOPPING CENTERS

7.1. Soluções de Gestão de Relacionamento de Clientes (CRM).

As soluções de Gestão de Relacionamento de Clientes (CRM) promovem melhor gerenciamento de contatos; colaboração entre equipes; maior produtividade; gerenciamento de vendas capacitado; previsão de vendas mais precisa; relatórios confiáveis; métricas de vendas aprimoradas; maior satisfação e retenção de clientes. Para tanto, é alimentado com um grande volume de Dados Pessoais.

Boas Práticas	Não vá por esse caminho...
i. assegurar que os Dados Pessoais que compõem o CRM são autorizados e processados mediante hipótese de Tratamento legítima, conforme Artigo 7º; **ii.** encriptar o CRM e toda e qualquer transferência de Dados Pessoais; **iii.** fazer uma avaliação de finalidade e necessidade. Eliminar o que não conjugar esses princípios; **iv.** limitar o acesso ao CRM àqueles que precisam acessá-lo em situações concretas; **vi.** investir em treinamentos dos representantes de vendas que usam o CRM; **vii.** investir em ferramentas que demonstrem os acessos ao CRM (trilha de auditoria, logs); **viii.** ter rotina de eliminação de dados e de renovação de Consentimento; **ix.** ter rotinas de auditoria e monitoramento do CRM, nas melhores práticas de mercado em LGPD. **x.** informar que o site usa cookies[1], incluindo a versão móvel (apps);	**i.** não manter registro dos acessos e motivos do Tratamento respaldado por hipóteses previstas no Artigo 7º; **ii.** não investir em criptografia de Dados Pessoais e medidas técnicas razoáveis de segurança da informação; **iii.** não ser transparente sobre o uso dos Dados Pessoais; **iv.** Tratamento excessivo sem finalidade e necessidade que o justifique ou necessárias ao serviço; **v.** permitir o acesso ao CRM sem devido treinamento; **vi.** não prever prazo justificável de manutenção de Dados Pessoais; **vii.** não ter formalizado, mediante contrato, obrigações e responsabilidades do gestor do CRM; **viii.** não realizar auditorias periódicas nas funcionalidades e compliance do CRM.

[1] Cookies coletam o comportamento em seu site, ajudando os profissionais de marketing a entenderem o que os clientes estão fazendo naquela página e como adaptar a sua estratégia de marketing aos seus visitantes. Isso não apenas melhora a eficácia do processo, mas também a experiência do usuário. No entanto, os clientes agora devem saber que seu comportamento está sendo monitorado, e o consentimento é necessário. Tenha um aviso de isenção em seu site, mas torne a desativação de cookies uma opção disponível. Ou então, você pode simplesmente perguntar se eles consentem em usar o seu site com os cookies ativados.

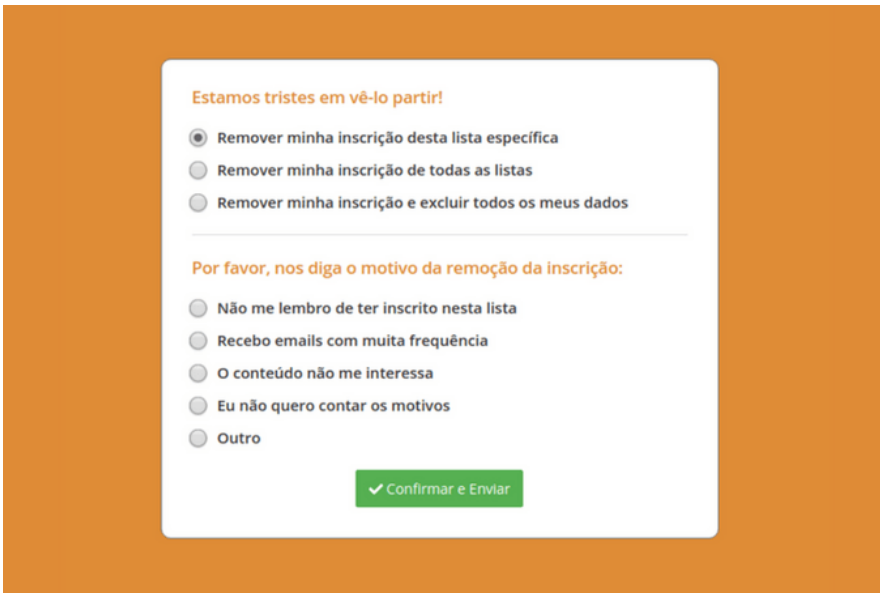
7.2. Marketing e Campanhas Promocionais

A LGPD é uma ótima oportunidade para que os profissionais de marketing façam o que fazem de melhor - criar campanhas direcionadas a clientes que se identificam com a marca e seus valores – já que o Consentimento, que não pode ser genérico, sob pena de nulidade, é dado após a ciência do tipo de informação que o Shopping Center detém e as finalidades para as quais são usados.

É preciso demonstrar que os dados de um indivíduo estão sendo tratados com respeito e mantidos com segurança.

Boas Práticas	Não vá por esse caminho...
i. disponibilizar e destacar, de forma clara, os termos da Política de Privacidade; **ii.** facilidade para a Eliminação de Dados Pessoais e revogação do Consentimento (Vide Figura 1); **iii.** pedir e ter meios para comprovar o Consentimento do Titular; **iv.** não presumir o Consentimento ou confundir atitudes do titular como tal; **v.** prezar pela clareza e transparência das informações sobre o tratamento de dados ao titular; **vi.** validar os termos da ação ou campanha com a equipe responsável por LGPD; **vii.** mapear públicos e direcionamento de campanhas por meio de perfis anonimizados; **viii.** dar descontos, benefícios, ações de fidelização que impliquem no registro do Consentimento.	**i.** não envolver especialistas em LGPD no lançamento de uma campanha de marketing ou ações promocionais; **ii.** ser evasivo, ambíguo, pouco claro nos termos de uso e políticas de privacidade; **iii.** dificultar ou tornar onerosa a eliminação de dados pessoais; **iv.** usar dados pessoais de campanhas ou ações anteriores sem a avaliação se o Consentimento foi concedido ou está válido; **v.** comprar Banco de Dados sem que haja o cuidado de verificar que todos os Dados Pessoais que o compõe foram obtidos por meios legítimos; **vi.** assumir o Consentimento por meios tácitos ou não expressos; **vii.** não renovar o Consentimento quando o escopo da ação de marketing ou promoção for ampliada e requerer o uso de Dados Pessoais;

Figura 1



Fonte: https://villetarget.com/blog/gdpr-na-automacao-de-marketing/. Acesso em 1 jul. 19.

7.3. Cadastro de Lojistas

Apesar do cadastro de clientes realizados pelas lojas do Shopping Center ser de responsabilidade do próprio lojista, que também está obrigado aos termos da LGPD, é importante inserir nos contratos de aluguel, bem como todos os compromissos celebrados entre o Shopping Center e o lojista (ex: promoções, ações de marketing conjuntas), cláusulas que imponham a responsabilidade aos lojistas de tratarem os Dados Pessoais nos termos da lei e de ressarcir o Shopping Center, caso venham a ocorrer danos causados em virtude de violações à lei ou inadimplemento de suas obrigações.

Basta imaginar a seguinte situação: Lojista, integrante de uma rede, com milhões de clientes em seus Bancos de Dados, sem controles específicos para o Tratamento de Dados Pessoais, vaza dados de cartão de crédito. Após investigação das autoridades, fica comprovado que o vazamento ocorreu na loja de determinado Shopping Center. As demais lojas da rede não tiveram esse tipo de problema e seguem com suas atividades normais.

Para o consumidor, pelo princípio da aparência, o tratamento é realizado pelo Shopping Center. Caso haja um vazamento de Dados Pessoais, usos indevidos, não respaldados por finalidade e hipótese legítima, por um lojista, o Shopping Center pode sofrer danos reputacionais, mesmo sendo capaz de demonstrar que não tem qualquer ingerência ou participação no incidente e nas atividades do lojista. Afinal, para o consumidor, melhor comprar em outro Shopping Center, que não teve nenhum problema.

Nos termos da LGPD, o Titular também poderá pedir explicações sobre decisões automatizadas que sejam tomadas a seu respeito. Lojistas que utilizam inteligência artificial para realizar diversos serviços, como rankings, classificações, perfis para segmentar o público alvo, poderão ter que fornecer explicações aos clientes sobre essas decisões automatizadas, pois podem não estar de acordo com a conclusão dessas decisões, tornando assim a segmentação do público alvo para os lojistas uma etapa a ser alinhada em compliance com a LGPD.

7.4. Relações de Trabalho e Emprego

O Shopping Center tem empregados e trata seus Dados Pessoais e, eventualmente, de seus dependentes, caso conceda benefícios.

Embora a LGPD autorize o Tratamento de Dados Pessoais de empregados e prestadores de serviços (Artigo 7°, incisos V e IX) para a legítima execução dos contratos, indispensáveis ao cumprimento de obrigações legais ou regulatórias pelo empregador (ex: envio de dados pessoais dos empregados ao Ministério do Trabalho e Emprego, INSS e CEF etc.); e em benefício do próprio empregado, é importante revisar sob a ótica da LGPD os atos praticados durante o processo de recrutamento e seleção, durante a vigência e término dos contratos de trabalho e nas terceirizações.

7.4.1. Recrutamento e Seleção

Boas Práticas	Não vá por esse caminho...
i. solicitar e registrar o Consentimento do candidato e informá-lo de maneira clara que seus Dados Pessoais serão utilizados para recrutamento, avaliação e seleção; **ii.** caso o candidato não seja contratado, eliminar os seus Dados Pessoais, ressalvadas as hipóteses de obrigação legal de conservá-los, ou questionar e pedir o Consentimento para armazenar os Dados Pessoais para futuras oportunidades; **iii.** orientar que apenas a área de Recursos Humanos pode receber currículos e que as demais devem eliminá-los de suas bases; **iv.** compartilhar currículos apenas com o Consentimento dos candidatos, ainda que para empresas do mesmo grupo econômico.	**i.** usar os Dados Pessoais de candidatos para finalidades distintas do processo de recrutamento e seleção; **ii.** ser evasivo, ambíguo, pouco claro nos termos de uso e políticas de privacidade para o uso de Dados Pessoais ao longo do processo de recrutamento e seleção; **iii.** compartilhar os currículos com outras empresas, ainda que do mesmo grupo econômico; **iv.** usar Dados Pessoais com caráter discriminatório e/ou informações pretéritas do candidato (ex: background checks, existência de ações trabalhistas por ele ajuizadas) como elemento capaz de definir sua contratação ou não, já que, nos termos da LGPD, Dados Pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo (Art. 21).

7.4.2. Contrato de Trabalho

Boas Práticas	Não vá por esse caminho...
i. dar ciência ao empregado do uso dos seus Dados Pessoais, autorizando-o para a realização de todas as ações relacionadas ao seu contrato de trabalho. **ii.** incluir o Consentimento do empregado, no contrato de trabalho, desde que em cláusula individualizada e devidamente destacada, bem como deve ser expresso e com finalidade determinada, sendo nulas disposições genéricas; **iii.** comunicar todas as alterações relacionadas ao Tratamento de Dados Pessoais; **iv.** Como a LGPD será aplicada independentemente da época em que a empresa teve acesso aos Dados Pessoais, para evitar o risco de indenizações quanto ao Tratamento pelo empregador que ultrapasse o cumprimento das determinações legais decorrentes do vínculo empregatício, recomenda-se obter autorização dos empregados para o Tratamento desses dados, especificando finalidade, forma e duração do tratamento, possíveis compartilhamentos e os direitos do empregado conforme estabelece a lei (Artigo 8º).	**i.** não destacar cláusula de proteção de dados, como obrigação, no contrato de trabalho; **ii.** não requerer ou presumir o Consentimento do empregado, em situações que o mesmo é necessário; **iii.** não ser transparente com as informações dos empregados; **iv.** vender informações de empregados; **v.** não eliminar informações de ex-empregados, após transcorridos prazos prescricionais; **vi.** violar direitos de proteção de dados e privacidade de empregados; **vii.** não considerar fins e hipóteses legítimas de Tratamento de Dados Pessoais; **viii.** assediar o empregado para que este dê seu Consentimento para determinada situação concreta.

7.4.3. Término do Contrato de Trabalho

Encerrada a relação de trabalho, seja por iniciativa do empregado ou da administração do Shopping Center, os Dados Pessoais do empregado devem ser eliminados, salvo nas hipóteses de obrigação legal de conservar tais documentos, para atendimento, por exemplo, de fiscalizações e ações trabalhistas.

7.4.4. Terceirização

Na terceirização de serviços, é preciso obter Consentimento dos empregados, por escrito, para que a empresa faça o tratamento dos seus dados, sobretudo quando for transmiti-los a terceiros (tomadores de serviço), em decorrência da atividade realizada, ou mesmo por exigências legais e contratuais, especificando de maneira clara quais dados serão repassados e para qual finalidade.

Além do Consentimento do empregado, é recomendável que as empresas criem obrigações específicas em seus contratos comerciais, de acordo com as exigências impostas pela LGPD no Tratamento.

7.5. Área de Tecnologia e Informação (TI)

Entre ameaças de crimes cibernéticos, vazamento de dados e a necessidade de estratégias específicas de monitoramento e implementação, será ainda mais importante utilizar soluções seguras e personalizadas para atender às exigências do regulamento e a confiança dos consumidores.

Boas Práticas	Não vá por esse caminho...
i. Promover auditoria completa do sistema de segurança atual; **ii.** mapeamento de processos e de responsáveis pela sua efetividade; **iii.** treinamentos a qualquer pessoa que lide com informações, ressaltando os riscos e noções de segurança da informação e proteção de dados. Isso inclui empregados, terceirizados, operadores dos sistemas de CRM, controle de portaria; **iii.** Plano de contingência: a LGPD exige que as organizações denunciem violações de dados no menor tempo possível. Todos sabem como agir em um incidente de segurança? Existem meios para responder a um incidente? **iv.** press release pronto para dar satisfação ao público e mitigar riscos de imagem.	**i.** adiar ou ignorar a importância da segurança da informação no escopo da LGPD; **ii.** não investir em ferramentas e arquitetura de sistemas de TI; **iii.** não mapear o ciclo de vida de Dados Pessoais sob Tratamento do Shopping Center; **iv.** não identificar as fragilidades de segurança; **v.** não ter plano de contingência preparado e protocolos de segurança a serem seguidos, caso ocorram incidentes; **vi.** não realizar treinamentos periódicos, a todos que lidam com Dados Pessoais, nos riscos e ameaças sob a ótica de TI.

7.6. Uso do Wi-Fi do Shopping

Os Shoppings Centers que disponibilizam aos consumidores, ou seja, aos Titulares de Dados Pessoais, a comodidade do uso do wi-fi, devem primar pela transparência na forma como suas informações serão tratadas.

Respeitar a privacidade dos usuários, trabalhar apenas com dados coletados de forma segura e legítima e, principalmente, prover experiências positivas para aos visitantes do Shopping Center são cuidados essenciais para o cumprimento da LGPD no oferecimento dessa comodidade.

Boas Práticas	Não vá por esse caminho...
i. elaborar termos de uso e de privacidade claros, detalhando as finalidades e usos dos dados; **ii.** requerer e arquivar o Consentimento para o uso do wi-fi; **iii.** primar pela coleta mínima de informações necessárias ao uso do wi-fi. Por exemplo, não é necessário coletar a orientação sexual, profissão para o uso do wi-fi;	**i.** coletar e armazenar Dados Pessoais sem que os usuários do wi-fi fiquem sabendo; **ii.** termos de uso e de privacidade genéricos, pouco claros, que podem levar o Titular a erro ou a vícios em seu Consentimento; **iii.** coleta excessiva de informações, que, para o uso do wi-fi, são totalmente dispensáveis e que não têm qualquer finalidade legítima.

7.7. Câmeras e Sistemas de Segurança

As imagens e os dados biométricos eventualmente captados por câmeras e sistema de segurança são dados pessoais, na medida que são passíveis de identificar um indivíduo, ainda que desconhecidos seu nome, identidade e demais informações de seu perfil.

Isso se justifica no termo "identificável", do Art. 1º da LGPD. Qualquer um que visualize as imagens ou cruze dados faciais, biométricos com uma base de dados, pode identificar o indivíduo em questão.

Nessa situação concreta, assumindo que as câmeras e sistemas de segurança de um Shopping Center têm como finalidades principais a proteção patrimonial, a prevenção e repressão de infrações penais (ex: furto, pilhagem, saques) e até mesmo a vida daqueles que o frequentam, existe legítimo interesse para o tratamento, que não requer o consentimento dos titulares, e se fundamenta nos termos do Art. 7º, inciso 4º, da LGPD.

Contudo, independentemente do consentimento, os princípios da LGPD devem ser observados no tratamento de dados provenientes de câmeras e sistemas de segurança, além de adotadas medidas de prevenção e boas práticas que coíbam vazamento e uso desalinhado com os fins legítimos de proteção ao patrimônio e segurança dos titulares.

Nesse sentido, para cumprimento da LGPD, o Tratamento de câmeras e sistemas de segurança requer um detalhamento nas políticas da administração do Shopping Center quanto ao prazo de retenção e de eliminação de dados alinhados com os fins legítimos que justificaram o tratamento.

Se o serviço é prestado por terceiros, estes serão Operadores, em relação à administração do Shopping Center. Nessa hipótese, é imperativo que seja formalizado um contrato entre prestador de serviços e a administração do Shopping Center, para que fiquem claras as regras de responsabilidade e solidariedade, caso haja qualquer incidente que implique em danos e direitos a indenização.

7.8. Estacionamento

O Tratamento de dados coletados no escopo do estacionamento do Shopping Center segue a mesma lógica do tratamento das imagens de câmeras e sistemas de segurança, pois, em regra, também são dados identificáveis e que seguem o mesmo princípio de segurança e proteção patrimonial.

Sendo assim, seguem valendo as orientações de observância aos princípios da LGPD; adoção de medidas de prevenção e boas práticas que coíbam vazamento e uso desalinhado com os fins legítimos que deram origem ao Tratamento; e de detalhamento nas políticas da administração do Shopping Center quanto ao prazo de retenção dos dados e de eliminação dos mesmos alinhados com os fins legítimos que justificaram o tratamento.

Se terceirizado, a recomendação de formalização de contrato entre prestador de serviços e a administração do Shopping Center, com regras de responsabilidade e solidariedade, também se aplica.

7.9. Creches, Espaço Mãe e Recreação de Crianças e Adolescentes

A LGPD, em seu Artigo 14, determina que Dados Pessoais devem ser processados de acordo com os princípios de melhor interesse da criança ou do adolescente e o condiciona ao Consentimento de um dos pais ou responsáveis legais.

Boas Práticas	Não vá por esse caminho...
i. Tratamento de Dados Pessoais de Crianças e Adolescentes apenas mediante o Consentimento dos pais ou responsáveis legais, que deve ser registrado, mediante meios técnicos disponíveis; **ii.** observar questões do Consentimento dos menores e a própria tutela do direito sobre esse grupo (Art. 17 – Estatuto da Criança e do Adolescente); **iii.** Tratamento limitado a fins legítimos e observado o princípio do melhor interesse da criança e do adolescente; **iv.** observância estrita ao princípio da necessidade dos Dados Pessoais tratados e, sempre que possível, promover sua Anonimização; **v.** políticas e termos de uso claros, diretos e acessíveis ao Usuário. Deve ser levado em consideração que os documentos dialogam tanto com os responsáveis como com as próprias crianças, e que precisam transmitir exatamente quais dados serão compartilhados; **vi.** investimento em solução técnica que seja capaz de demonstrar os melhores esforços para a obtenção e registro do Consentimento. Por exemplo: o cadastro de cartão de crédito, comprovantes de pagamento de contas ou até criar um filtro que demande uma foto do responsável legal segurando o RG do menor, similar ao que bancos pedem para a criação de contas online.	**i.** não adotar nenhuma medida para verificação se Dados Pessoais de Crianças e Adolescentes estão sob Tratamento do Shopping Center; **ii.** políticas de privacidade e termos de uso com frases dúbias, longos períodos e contradições, que podem induzir o Titular a erro ou confundi-lo; **iii.** Tratar Dados Pessoais de Crianças e Adolescentes em excesso, sem sua ciência, de forma clandestina e sem fins legítimos; **iv.** não promover a Eliminação de Dados Pessoais de Crianças e Adolescentes, que não contam com Consentimento e hipótese de Tratamento legítima; **v.** não considerar os melhores interesses das crianças e adolescentes; **vi.** violar as disposições do Estatuto da Criança e do Adolescente no escopo do Tratamento.

8. ENCARREGADO – DATA PROTECTION OFFICER DO SHOPPING CENTER

O Capítulo IV, da LGPD, "Dos Agentes de Tratamento de Dados Pessoais", dedica a Seção II e o art. 41 ao "Encarregado pelo Tratamento dos Dados Pessoais".

O Shopping Center deverá indicar, em seu site, a identidade e os contatos do seu Encarregado, que poderá ser uma pessoa física ou jurídica, de forma clara e objetiva.

Suas atribuições, nos termos da lei, consistirão em:

i. aceitar reclamações e comunicações dos Titulares, prestar esclarecimentos e adotar providências;
ii. receber comunicações da ANPD e adotar providências;
iii. orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de Dados Pessoais; e
iv. executar as demais atribuições determinadas pelo Shopping Center ou estabelecidas em normas complementares.

A LGPD faculta à ANPD, entre outras atribuições, editar normas e procedimentos para regulamentação da LGPD, interpretar a LGPD, fiscalizar e aplicar as sanções, e, ainda, ampliar atribuições do Encarregado ou até mesmo dispensar sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

No Brasil, como a LGPD ainda não entrou em vigor, não existem diretrizes, precedentes judiciais ou uniformidade nas práticas de mercado em relação ao perfil do profissional que atuará como Encarregado ou seu vínculo com o Controlador.

Na Europa, na vigência do GDPR, já existe algum posicionamento em relação ao perfil, habilidades e forma de contratação do Data Protection Officer (DPO), figura análoga ao Encarregado, da legislação brasileira.

Segundo as diretrizes do European Data Protection Supervisor (EDPS)[2], item 3.2, o DPO deve ser selecionado de acordo com seu conhecimento em leis relativas à proteção de dados e conjunto de habilidades que o capacitam para cumprir as atividades previstas no GDPR.

O EDPS enfatiza que dois (2) elementos são fundamentais àqueles que ocuparão o cargo de DPO: (i) conhecimento adequado do perfil do controlador de dados, da sua estrutura e funcionamento; e (ii) expertise em proteção de dados.

O GDPR permite, ainda, o acúmulo de funções de DPO[3] com outras desempenhadas pelo empregado do controlador, desde que não haja qualquer tipo de conflito de interesses.

A LGPD não faz qualquer menção aos requisitos formais do relacionamento do Encarregado com o Controlador, sendo cabível, como é na Europa, a terceirização do serviço. Em verdade, todas as atividades do encarregado, demonstram muito mais um caráter de serviço do que a atividade de uma única pessoa[4].

[2] Vide https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf. Acesso em 12 jul. 2019.
[3] Vide Art. 38:6 do GDPR.
[4] PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018. São Paulo: Saraiva Educação, 2018.

9. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: NO QUE CONSISTE E QUAL A SUA IMPORTÂNCIA?

O Relatório de Impacto à Proteção de Dados Pessoais é uma ferramenta para garantir e demonstrar conformidade com a LGPD.

Ele consiste, basicamente, em uma documentação que descreve os processos de Tratamento de Dados Pessoais que podem gerar algum risco aos direitos dos Titulares, além das medidas e mecanismos empregados para mitigar esses riscos.

A construção do relatório parte do detalhamento de todos os processos de Tratamento pelos quais os Dados Pessoais passam durante o seu ciclo de vida na operação, assim como das bases legais necessárias e as medidas de segurança adotadas.

A descrição detalhada do ciclo de vida dos Dados Pessoais, associada à consulta e à colaboração com os Agentes de Tratamento envolvidos, permite identificar os pontos de fragilidade da operação, que podem representar algum risco aos direitos dos Titulares.

Assim, é feita uma avaliação desses riscos, a partir da qual são identificadas as medidas necessárias para a sua contenção, que devem ser implementadas e testadas.

Um bom Relatório de Impacto à Proteção de Dados Pessoais contém, por exemplo:

i. as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da LGPD;
ii. as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da LGPD e políticas internas;
iii. o parecer da área responsável pelo registro e controle dos mecanismos de controle e cumprimento da LGPD;
iv. plano de ação para fragilidades e deficiências, bem como sugestões de melhoria contínua.

10. CONSIDERAÇÕES FINAIS

Com a LGPD, o Brasil entrou no rol de países que possuem uma Lei Geral de Proteção de Dados.

A nova lei surge como um divisor de águas, exigindo um giro conceitual na forma como os Shopping Centers se relacionam com Dados Pessoais. Mais que empoderar as pessoas físicas quanto às informações que lhes dizem respeito, a LGPD se insere em um cenário de transparência e ética no mundo dos negócios, que, cada vez mais, dependem de meios digitais.

Para que todos levem os seus termos a sério, foram previstas penalidades severas, que serão evitadas por meio de boas políticas de dados e termos de uso, que garantam a atuação de todos os Controladores dentro das novas diretrizes, alinhadas com o cenário mundial.

A responsabilidade por essas questões passa a ser de todos que interagem com Dados Pessoais, em nome ou em benefício do Shopping Center, que deverá prestar contas, demonstrar diligência e ressarcir eventuais violações ou inobservância aos termos da LGPD.

A administração do seu Shopping Center está preparada para assumir a responsabilidade perante clientes? Considera um dano de imagem decorrente de perda, roubo ou vazamento de dados? Não? Então se prepare, consulte e conte com ajuda de profissionais especializados em LGPD.

Essa cartilha não se destina a esgotar o tema e/ou substitui o auxílio a profissionais especializados nos termos da LGPD e Direito Digital. Esperamos que as orientações aqui dispostas contribuam para a continuidade do sucesso do Shopping Center associado, em cumprimento às normas e leis aplicáveis.

Pensou shopping pensou ABRASCE

ABRASCE

www.abrasce.com.br

abrasce abrasceshoppingcenters abrasceoficial

company/abrasce CanalAbrasce