ABADI

Manual Operacional da LGPD

PARA ADMINISTRADORAS DE CONDOMÍNIOS E IMÓVEIS

Lei nº 13.709/2018

Versão 1.0

Manual Operacional da LGPD

PARA ADMINISTRADORAS
DE CONDOMÍNIOS E IMÓVEIS

A Associação Brasileira das Administradoras de Imóveis (ABADI) se dedica há 46 anos em reunir empresas de administração imobiliária em prol de um mercado mais saudável, ético e próspero. Neste caso, propagar conhecimento sem fins lucrativos ou comerciais nos permite ser uma fonte isenta e confiável para quem deseja entender melhor a atividade.

Dentre as missões da ABADI está a incansável preocupação em desenvolver materiais e protocolos que poderão servir como ferramentas para o melhor desempenho das atividades das nossas associadas, objetivando uma prestação de serviço qualitativa aos seus respectivos clientes.

Com imagem sólida e positiva no mercado, a ABADI é referência tanto para a sociedade quanto para a opinião pública, representando mais de 85% do mercado imobiliário do Rio de Janeiro.

Propósito do documento

A finalidade do Manual de Boas Práticas da Lei Geral de Proteção de Dados (LGPD) é relacionar as principais diretrizes e recomendações para que administradoras de imóveis e condomínios compreendam, na visão da ABADI, o impacto da Lei em suas atividades e saibam como operacionalizar todas as suas atribuições da forma correta, sanando dúvidas e eventuais dificuldades.

Este material foi idealizado pela diretoria da ABADI e redigido em conjunto com colaboradores das empresas associadas e especialistas na matéria. Espera-se que este documento auxilie no entendimento inicial os efeitos da Lei sobre as operações das empresas.

COORDENAÇÃO

Rafael Thomé | Presidente da ABADI
Fernando Schneider | Vice-presidente da ABADI
Marcelo Borges | Diretor de Condomínio e Locação da ABADI

Agradecemos às administradoras associadas, que disponibilizaram seus colaboradores para este projeto.

CO-AUTORES

Claudio Latta (Novi Adm)
Gabriela Duarte (BAP)
João Eduardo da Costa (Estasa)
Juliana Tancredo (Apsa)

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

Nos últimos anos, houve um grande avanço da tecnologia e com ela o aumento do fluxo de informações, seja online ou off-line. A quantidade e qualidade da coleta de dados pessoais cresceram exponencialmente, o que permite que aquele que detém esses dados possa facilmente utilizá-los para determinar padrões comportamentais, hábitos de uso e serviços, entre outros.

Diante deste cenário, mesmo com a existência de diferentes leis que tratam de dados pessoais, viu-se a necessidade de se estabelecer uma relação mais adequada e transparente entre os cidadãos e empresários no que se refere ao manuseio dos dados pessoais, o que resultou na edição de leis de proteção de dados pessoais em vários países do mundo.

Também conhecida pela sigla "LGPD", a Lei Geral de Proteção de Dados do Brasil, sancionada em agosto de 2018, estabelece regras para que se realize a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, garantindo maior proteção aos direitos fundamentais de liberdade e privacidade do titular do dado, além de prever as devidas penalidades em hipótese de descumprimento.

"Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.'

2. Bases legais

O art. 7° da Lei Geral de Proteção de Dados dispõe sobre as chamadas "bases legais". Trata-se de dez hipóteses que irão condicionar a realização de coleta e posterior tratamento dos dados pessoais.

As bases legais, portanto, irão regulamentar e legitimar o armazenamento, tratamento e compartilhamento dos dados. Desse modo, vemos que a administradora necessariamente deverá estar pautada em uma ou mais bases para tratar dados pessoais, quais sejam:

• Consentimento do titular (art. 7, I, LGPD) - O titular dos dados, através de manifestação livre e inequívoca, deve concordar expressamente com o tratamento de seus dados pessoais.

• Legítimo Interesse (art. 7, IX, LGPD) - Trata da vontade do controlador ou da sociedade em se beneficiar de forma legal com o tratamento de dados pessoais, que está subordinado a quatro itens:

- Somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados (art. 10, § 1º,LGPD);
- O controlador deve adotar medidas para garantir a transparência do tratamento de dados (art. 10, § 2º, LGPD);
- As legítimas expectativas do titular devem ser respeitadas (art. 10, II, LGPD);
- Os princípios da LGPD e os direitos do titular devem ser assegurados (art. 10, II, LGPD).

• Cumprimento de obrigação legal ou regulatória (art. 7, II, LGPD) - Trata-se de cumprimento de determinação legal preexistente ou para garantir a ordem e segurança social.

• Tratamento pela administração pública (art. 7, III, LGPD) - Possui a finalidade específica de viabilizar a execução de políticas públicas instituídas conforme prevê a legislação.

• Realização de estudos e de pesquisas – (art. 7, IV, LGPD) Tratamento de dados voltado para pesquisas que tenham como base a saúde pública ou programas governamentais.

• Execução ou preparação contratual (art. 7, V, LGPD) - Legitima-se na necessidade para execução de um contrato ou de procedimentos preliminares relacionados a um contrato em que o titular dos dados figurará como integrante.

• Exercício regular de direitos (art. 7, VI, LGPD) - Viabilização do exercício regular de direito, incluindo contraditório, ampla defesa e devido processo legal.

• Proteção da vida e da incolumidade física (art. 7, VII, LGPD) - Esta base legal trata do tratamento de dados feito com o objetivo de tutelar a vida ou a incolumidade física do titular dos dados ou de terceiros.

• Tutela de saúde do titular (art. 7, VIII, LGPD) - A LGPD também autoriza o tratamento de dados para a tutela da saúde, desde que realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

• Proteção de crédito (art. 7, X, LGPD) - O tratamento de dados em função da manutenção e proteção de crédito dispensam consentimento e está autorizado, desde que seja realizado negócio jurídico de interesse do titular.

3. Fundamentos da LGPD

Alinhada com as garantias trazidas pelo art. 5° da Constituição Federal de 1988 e com o objetivo de tutelar os direitos fundamentais do cidadão, o art. 2º da LGPD traz os fundamentos para a proteção de dados e a privacidade, quais sejam:

• O respeito à privacidade;
• A autodeterminação informativa;
• A liberdade de expressão, de informação, de comunicação e de opinião;
• A inviolabilidade da intimidade, da honra e da imagem;
• O desenvolvimento econômico e tecnológico e a inovação;
• A livre iniciativa, a livre concorrência e a defesa do consumidor; e
• Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4. Aplicação da LGPD

A Lei se aplica a qualquer operação de tratamento de dados realizada por pessoa natural ou por pessoa jurídica, de direito público ou privado, que possua estabelecimento no Brasil, e/ou oferece produtos e serviços ao mercado brasileiro, e/ou coletam e tratam dados de pessoas que estejam no país, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- A operação de tratamento seja realizada no território nacional;
- A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
- Os dados pessoais objeto do tratamento tenham sido coletados no território nacional;

5. Programa de governança em privacidade

A Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) [14], em sua Seção II, Das Boas Práticas e da Governança, informa, no Art. 50 § 2º sobre as características mínimas de um Programa de Governança em Privacidade – PGP, conforme apresentado na Figura 1.

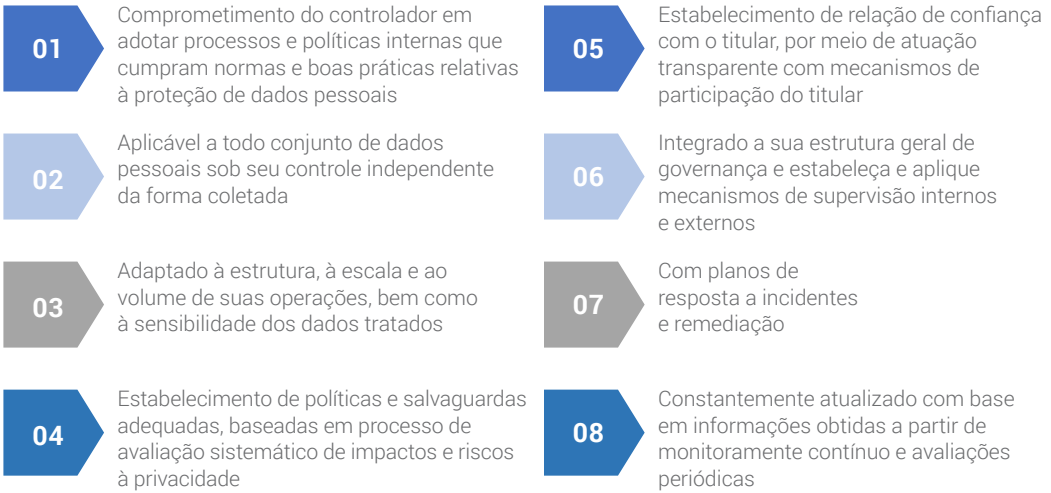


Figura 1. Características Mínimas de um Programa Gerenciamento de Privacidade - LGPD

Diante das características, entendemos ser necessário que cada administradora associada conte com um Programa de Governança em Privacidade.

Destacamos os principais atores das relações que envolvem o tratamento de dados:

1 - No papel central, por sua importância, tem-se o **titular**, qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa.

2 - A seguir, o **controlador**, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador pode exercer diretamente o tratamento dos dados. Mas pode, também, designar um operador;

3 - O **operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Ambos, controlador e operador, recebem a nomeação de "agentes de tratamento";

4 - O **encarregado** corresponde a uma pessoa natural inequivocamente investida nessa função (que, na legislação europeia, corresponde ao Data Protection Officer - DPO). Sua incumbência é de fazer a intermediação entre o titular e os agentes de tratamento, mas também entre estes agentes e a Autoridade Nacional de Proteção de Dados – ANPD;

5 - Finalmente, a **Autoridade Nacional de Proteção de Dados - ANPD** tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados.

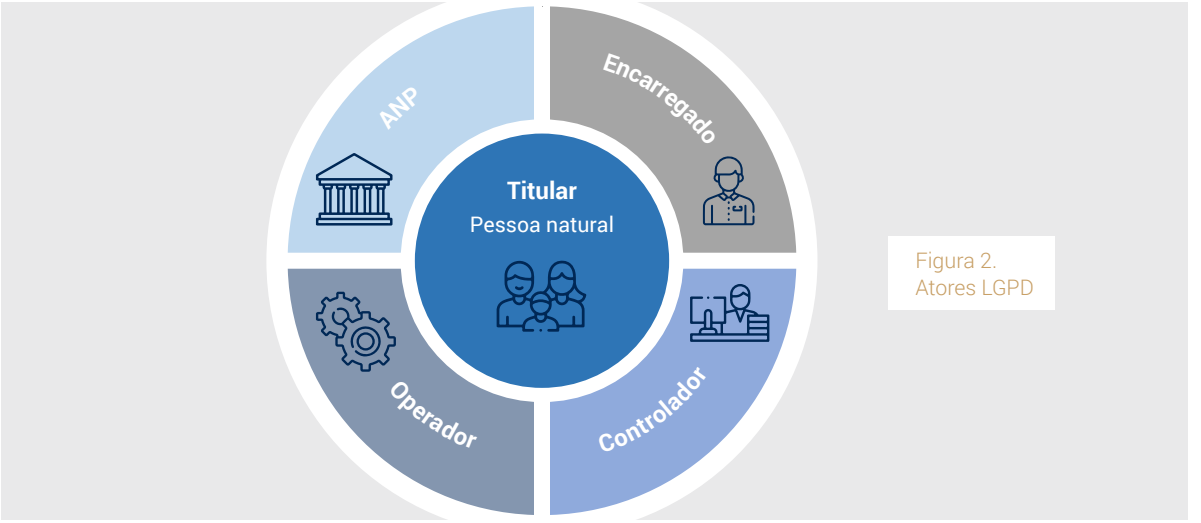


Figura 2.
Atores LGPD

Vale ressaltar que, ao contrário de um projeto que tem início, meio e fim, um programa estabelece uma metodologia abrangente que influenciará permanentemente nos processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade. Pode-se, entretanto, criar projetos para se alcançar os objetivos do programa. Na criação de projetos para se alcançar objetivos do programa, deve-se selecionar a metodologia mais adequada à realidade institucional. Após a escolha da metodologia é necessário definir:

- Os objetivos, as metas e os indicadores;
- Os líderes responsáveis por cada frente de atuação do projeto (interação com o cidadão, operações de TI, segurança, jurídico, operadores, entre outros); e
- Canais de comunicação com os líderes, cidadãos, com os operadores e com a Autoridade Nacional de Proteção de Dados - ANPD.

Recomenda-se ainda criar modelos padronizados para obtenção de respostas que subsidiarão reportes para a alta administração.

6. Estruturação

O programa foi estruturado nas seguintes etapas, conforme Figura 3, e serão descritas e detalhadas no próximo capítulo:

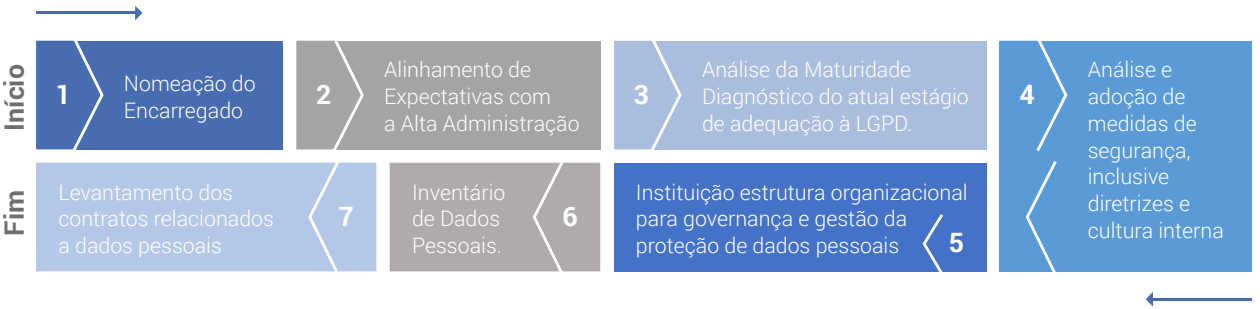
Figura 3. Etapas Programa de Governança em Privacidade – PGP

Etapas do Programa de Governança em privacidade

O programa de governança em privacidade está dividido em etapas a serem executadas por cada administradora, dependendo de sua capacidade de desenvolvimento do projeto.

Iniciação e Planejamento

A etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Com isso em mente, essa etapa é constituída pelos marcos apresentados na Figura 4, que serão detalhados a seguir.



Recomenda-se que o início seja dado pela nomeação do Encarregado, que conduzirá a instituição em conjunto com o Comitê de Governança Digital. O encarregado é um dos membros do Comitê de Governança Digital, que tem como objetivo deliberar sobre os assuntos relativos à implementação das ações digitais e ao uso de recursos de tecnologia da informação e comunicação.

O início também deve incluir a criação de uma estrutura organizacional para compor o conhecimento de dados pessoais em toda administradora, além de supervisionar as três etapas de ação para criar e manter o Programa de Governança em Privacidade (PGP).

A. O Encarregado

A indicação do encarregado deve acontecer no início do PGP. O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Entre as competências de um encarregado apresentadas na LGPD, pode-se citar:

01 Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências

02 Receber comunicações da autoridade nacional e adotar providências

03 Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

04 Apoiar a definição das diretrizes de construção do inventário de dados pessoais relativas ao registro das operações de tratamento de dados pessoais determinado pelo art. 37 da LGPD

05 Conduzir ou aconselhar a elaboração de relatório de impacto à proteção de dados pessoais, de acordo com casos previstos pela LGPD em que tal documento é necessário

06 Conduzir ou aconselhar a implementação de regras de boas práticas e de governança especificadas pelo art. 50 da LGPD

07 Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares

Figura 5. Competências Encarregado – LGPD

É importante que o encarregado tenha independência para determinar a aplicação de recursos e as ações necessárias, bem como o pronto de apoio das unidades administrativas no atendimento das solicitações de informações em relação às operações de tratamento de dados pessoais. Também deve ter amplo acesso a estrutura organizacional, investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir as lacunas encontradas.

É válido destacar que o apoio da alta administração é essencial para o sucesso do trabalho executado pelo encarregado, incluindo seu envolvimento nas decisões e recursos suficientes para pessoal, treinamento, entre outros.

O encarregado necessita, também, de autonomia e independência funcional para avaliação das atividades de tratamento de dados pessoais realizadas pelo órgão e um contínuo aperfeiçoamento por meio de treinamentos e capacitações realizadas com segurança da informação e proteção de dados pessoais.

Diante da nítida importância do encarregado para a implementação da LGPD e, consequentemente, para o PGP, a seguir é apresentada uma proposta de tópicos a serem abordados, analisados e tratados pelo encarregado. É recomendado que o trabalho a ser executado pelo encarregado também seja dividido em etapas e os seguintes passos são sugeridos:

1. Alinhamento de expectativas entre o encarregado e a alta direção da administradora;

2. Apresentação, para os colaboradores da empresa, do papel exercido pelo encarregado como relevante e influenciador;

3. Como o encarregado pode servir e agregar valor à administradora, dado o disposto na LGPD;

4. Confirmar e garantir aos colaboradores, enquanto representantes internos da ANPD, que seu papel deve ser uma assistência de grande valor e não um obstáculo;

5. Priorização e foco em melhorias, tendo consciência da estrutura, dos requisitos de dados pessoais, bem como da maturidade de compliance da administradora;

6. Lançamento e implementação de mecanismos para geração de relatórios internos de atividades de processamento de dados pessoais, sejam tais atividades novas, majoritárias ou com alterações;

7. Conclusão de um inventário de dados pessoais, destacado no início desta seção, com a lista dos principais serviços que utilizam dados pessoais da administradora;

8. Alcance de credibilidade e valor entre todos os colaboradores;

9. Instituição e coordenação, em conjunto com o Comitê de Governança Digital, de uma Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais.

10. Apresentação de minuta de política de privacidade aos gestores da empresa, com o comprometimento de revisar, conforme os apontamentos de melhorias sugeridos;

11. Projeção ou refinamento de uma nova estratégia de privacidade: um mapeamento do atual cenário e fornecimento de uma visão geral do orçamento necessário para, no mínimo, os próximos 12 meses, bem como a associação e o relacionamento aos pontos de atenção listados;

12. Neste início sugere-se concentrar em poucos assuntos, balanceando entre as áreas de maior risco e as mais simples do órgão, quanto à privacidade dos dados. Por exemplo, alternar entre o projeto com maior risco no que envolve dados pessoais e uma campanha de sensibilização para os colaboradores.

B. Alinhamento de Expectativas com a Alta Administração

Ao longo da etapa de Iniciação e Planejamento é importante ainda alinhar as expectativas com a alta administração, priorizando as ações mais urgentes, sem esquecer de mencionar os projetos e as estruturas da organização envolvidas. Considera-se como alta administração: diretoria, gestores, gerentes ocupantes de cargos de natureza especial. É importante destacar que o alinhamento com a alta administração e a priorização de ações urgentes guiam o estabelecimento da cultura de proteção de dados na instituição.

C. Maturidade da Organização

Outro ponto a se analisar é a maturidade da organização, observando fatores como a rastreabilidade de dados - estruturando-os e descrevendo as informações tratadas em cada sistema, a comunicação com o cidadão e a transparência (elaborando, por exemplo, a política de privacidade e termos de uso de serviços, bem como a comunicação sobre o uso de cookies).

D. Medidas de Segurança

Na etapa de Iniciação e Planejamento, medidas de segurança também devem ser analisadas e adotadas, revisando e propondo aprimoramento das diretrizes e cultura internas.

E. Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais

Recomenda-se ainda, como suporte para a estrutura do PGP, assim como para a realização das atividades do encarregado provenientes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, o estabelecimento de uma estrutura organizacional para governança e gestão da proteção de dados pessoais, de acordo com o porte da instituição.

F. Inventário de Dados Pessoais

Para obter um mapeamento dos dados pessoais utilizados pelo órgão, recomenda- se a realização de um inventário de dados, especialmente dos dados pessoais. Conforme o Guia de Elaboração de Inventário de Dados Pessoais, o Inventário de Dados Pessoais representa documento primordial no sentido de documentar o tratamento de dados pessoais realizados pela instituição. O inventário consiste em uma excelente forma de fazer um balanço do que a administradora faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

G. Levantamento de Contratos relacionados a Dados Pessoais

O levantamento dos serviços que tratam dados pessoais no Inventário de Dados viabiliza a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

7. Construção e Execução

Na etapa de construção de um programa de gerenciamento da privacidade, deve-se considerar os pontos de atenção listados na Figura 6.

Gerenciamento de direitos individuais

O gerenciamento de direitos individuais de dados é essencial para LGPD, como o direito de acessar os dados que um órgão ou entidade mantém sobre os indivíduos, bem como o direito de os atualizar. Os órgãos e entidades devem estar preparados para receber, realizar a triagem e responder consultas e reclamações, podendo sofrer penalidades por não responder de maneira oportuna.

Consentimento e rastreamento de preferência

Os cidadãos querem saber se as suas preferências estão sendo honradas. Para o órgão, estar posicionado para capturar consentimento e rastrear solicitações de preferências tanto dos titulares dos dados como dos agentes de tratamento ajuda a reduzir a probabilidade de problemas e aumenta a confiança do cidadão.

Redução de responsabilidade por violação

A redução da exposição pode ser feita por meio de medidas como, por exemplo, criptografia e anonimização de dados. Os dados devem ser mantidos apenas para sua finalidade.

Figura 6. Considerações Etapa de Construção e Execução

Logo, neste capítulo, os marcos a serem alcançados na etapa de Construção e Execução, apresentados na Figura 7, serão descritos e detalhados.

Figura 7. Marcos Etapa Construção e Execução

A. Políticas e práticas para proteção da privacidade do cidadão

Na construção de um PGP devem ser especificadas políticas e práticas para proteger a privacidade do cidadão, garantindo que todos os usos dos dados pessoais são conhecidos e adequados de acordo com as leis, bem como sua proteção contra mau uso ou revelação inadvertida ou deliberada. Além das políticas e práticas nas administradoras, papéis específicos dos responsáveis envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais devem ser colocados em prática, assim como a educação dos colaboradores em relação a políticas e práticas de proteção de privacidade e dos cidadãos em relação aos seus direitos quanto à privacidade da informação.

Informações como a finalidade e a base legal para tratamento de dados obtidas no inventário dos dados pessoais realizado na fase de Iniciação e Planejamento, são úteis na construção das operações de tratamento. Tais informações auxiliam na determinação dos detalhes do ciclo de vida dos dados pessoais. Por exemplo: a finalidade do tratamento, como, onde e por quanto tempo é o armazenamento, entre outros.

B. Cultura de segurança e proteção de dados e Privacidade desde a Concepção

A promoção de uma cultura de segurança e proteção de dados deve ser tratada na etapa de construção e execução de um PGP com o intuito de comunicar os objetivos, metas e indicadores utilizados, além de divulgar o papel da administradora como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos. As informações do PGP devem ser disponibilizadas de forma clara e eficiente, além de estarem facilmente acessíveis. Capacitação e treinamento devem ser oferecidos para que uma cultura de Privacidade desde a Concepção *(privacy by design)* seja instituída.

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Conforme o Guia de Boas Práticas da LGPD, tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais, listados a seguir:

1. Proativo e não reativo; preventivo, e não corretivo: A abordagem de Privacidade desde a Concepção (PdC) antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem, nem oferece soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram.

2. Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio: Busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

3. Privacidade incorporada ao projeto (design): A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

4. Funcionalidade total: A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade, permitindo funcionalidade total com resultados reais e práticos. Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.

5. Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados: Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.

6. Visibilidade e Transparência: A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança.

7. Respeito pela privacidade do usuário: Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

C. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

É ainda na etapa de Construção e Execução do PGP que o Relatório de Impacto à Proteção de Dados Pessoais - RIPD deve ser elaborado. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais. O RIPD visa descrever os 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.

D. Medidas e Política de Segurança da Informação e Política de Privacidade

Ainda na etapa de Construção e Execução do PGP, tem-se o desenvolvimento e/ou a atualização das diretrizes internas de proteção de dados pessoais. Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessária a retenção de determinados dados tratados e se é necessário revisar contratos. Desse modo, torna-se fundamental o desenvolvimento de uma política de segurança da instituição, bem como de uma política de privacidade de dados.

É necessária a elaboração de uma Política de Privacidade, que é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário. A Política de Privacidade, que faz parte do Termo de Uso, origina- se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informarem como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6º LGPD. Portanto, o documento é, ao mesmo tempo, um dever do controlador e um direito do titular. Assim, de acordo com o Guia de elaboração de Termo de Uso e Política de Privacidade, o serviço deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente e como os princípios da LGPD são atendidos:

• **Finalidade:** Obrigatoriedade de tratamento somente para fins legítimos, específicos, explícitos, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

• **Adequação:** Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

• **Necessidade:** Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

• **Livre acesso:** Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

• **Qualidade dos dados:** Critérios de qualidade dos dados, para garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

• **Transparência:** Critérios de transparência, para garantir, aos titulares, o fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

• **Segurança:** Critérios de segurança, para que se utilize medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

• **Prevenção:** Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

• **Não discriminação:** Critérios de não discriminação para garantir que não se realize o tratamento de dados para fins discriminatórios ilícitos ou abusivos;

• **Responsabilização e prestação de contas:** para que em cada tratamento de dados se possa demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

SUGERE-SE QUE UMA POLÍTICA DE PRIVACIDADE CONTENHA OS TÓPICOS APRESENTADOS NA LISTAGEM ABAIXO

1. Controlador
2. Operador
3. Encarregado
4. Quais dados são tratados
5. Como os dados são coletados
6. Qual o tratamento realizado e para qual finalidade
7. Compartilhamento de dados
8. Segurança dos dados
9. Cookies
10. Tratamento posterior dos dados para outras finalidades
11. Transferência internacional de dados

As medidas de segurança para a proteção dos dados pessoais devem ser implementadas na fase de Construção do Programa de Governança em Privacidade. Segurança desde a Concepção e a importância de se tomar medidas preventivas precisam ser consideradas, bem como a gestão dos riscos, a gestão de incidentes e a violação dos dados.

Por fim, mas não menos importante, os direitos dos titulares precisam ser gerenciados. Devem ser destacadas e elucidadas questões como a diferença entre o titular e o custodiante do dado pessoal, do ponto de vista da administradora, bem como as obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade.

E. Adequação de Cláusulas Contratuais

Durante a implantação do **Programa de Governança em Privacidade – PGP** surgem recomendações e necessidades de mudança contratuais, que precisarão ser avaliadas e/ou realizadas com os novos clientes em operação. As recomendações identificadas, não exaustivas, durante a confecção deste Guia, são:

1. Revisão de contratos com parceiros externos:

A revisão dos contratos já firmados e elaboração de minutas contratuais que servirão como referência para futuras parcerias comerciais é essencial. Contratos contém dados pessoais e sensíveis de clientes, por essa razão, recomenda-se que a revisão envolva todas as negociações realizadas com seus seguintes parceiros. Citamos alguns exemplos:

• Dos contratos com Birô especializados na emissão de boletos;
• Dos contratos com empresas terceirizadas na execução de sustentação de infraestrutura como:

Sustentação do circuito interno de TV;
Sustentação de central telefônica;
Sustentação da rede de dados;
Sustentação da infraestrutura de servidores;
Acervo de backups de dados;
Acervo externo de documentos físicos;

• Dos contratos de prestadores de serviço terceirizados, como: Vale Transporte; Seguradoras; Cartão VT e VA, na administração da folha de pagamento dos clientes condomínio;
• Dos contratos com os clientes locação, sendo eles proprietário e locatários;
• Do acervo de documentos clientes condomínio: RGI, convenções, regimento interno, regulamento, atas, editais de convocação, contratos de prestadores de serviço diversos do condomínio.
• Dos contratos com os clientes condomínio;
• Dos contratos de contratação dos funcionários cliente condomínio;

A fim de evitar qualquer tratamento de dados inadequado pelo operador e/ou controlador, conforme o caso, ou terceiros com quem compartilha os dados, a administradora deve ter a política de contratar apenas parceiros que adotem os padrões de proteção de dados exigidos pela LGPD, solicitando, à empresa com quem pretende estabelecer vínculo contratual, por exemplo, a apresentação de relatório de impacto à proteção de dados.

Neste contexto, recomenda-se que a administradora audite seus parceiros para verificar os procedimentos por eles adotados no tratamento de dados e as medidas de segurança implementadas. Note que essa auditoria não poderá ser apenas inicial, no momento da contratação, mas deverá ser realizada com determinada periodicidade que assegure que o parceiro continua adotando os padrões da LGPD. Tal periodicidade dependerá do tipo de tratamento realizado pelo parceiro, dos dados tratados, dentre outros fatores de riscos que devem ser levados em consideração pela empresa.

2. Contratos trabalhistas:

O empregado é controlador dos dados pessoais que serão objeto de tratamento, que é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.Logo, os contratos que tem por finalidade regular as relações trabalhistas deverão contar com a revisão e inclusão de cláusulas de resguarda na utilização e tratamento dos dados pessoais dos empregados da administradora.

Alguns dados que envolvem a relação trabalhista entre administradora/empregado são:

• Dados anteriores à contratação: perfil do candidato, currículo, histórico escolar.
• Dados da celebração do contrato: dados pessoais, residência, situação familiar, tipo sanguíneo;
• Dados durante a execução do contrato: jornada de trabalho, valor do salário, acidentes, doenças, situação conjugal;
• Dados após o fim do contrato: valor das verbas rescisórias, motivo do desligamento.
• Dados enviados aos órgãos públicos: convênios médicos, vale alimentação, órgãos trabalhistas.

Ainda sobre as relações de trabalho e a aplicação da LGPD pelas administradoras, merece destaque a imprescindibilidade de as empresas elaborarem um código de conduta. Tal documento definirá os papeis e responsabilidades dos envolvidos e, sobretudo, servirá como referência para o uso e manuseio correto dos dados que sejam coletados pela empresa.

Após a ampla divulgação do código de conduta elaborado, é recomendável que o empregador ofereça aos seus empregados os treinamentos e capacitações que condicionam o manuseio dos dados a que tem acesso. Feito isso, é igualmente aconselhável que os empregados assinem um termo de responsabilidade, onde atestarão que tomaram ciência das disposições legais em vigor.

No que concerne às relações de trabalho estabelecidas entre os condomínios administrados e os seus respectivos empregados, a administradora deverá se limitar a recomendar ao cliente que providencie a adequação de suas minutas à LGPD.

F. Abordagem geral sobre as penalidades

• Delimitações claras e objetivas das responsabilidades do controlador e operador;
• A forma que é realizada a coleta e o tratamento de dados;
• A existência da possibilidade de o titular acessar os seus dados coletados;
• A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
• A existência da possibilidade de revogação do consentimento dado pelo titular;
• O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
• As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

G. Termo de Uso

O Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele.

O Termo de Uso, como a Política de Privacidade, advém da consciência do controlador e operador ser transparente com o titular de dados pessoais e comunicar como as atividades de tratamento desses dados observam os princípios dispostos no artigo 6º da LGPD. Em cumprimento aos princípios da publicidade e da transparência, e a fim de assegurar aos cidadãos amplo acesso às informações, os termos devem ser regularmente atualizados a fim de refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares.

OS TÓPICOS QUE DEVEM CONSTAR NO TERMO DE USO ESTÃO LISTADOS NO QUADRO A ABAIXO: QUADRO 3 – TÓPICOS TERMOS DE USO.

1. Aceitação dos Termos e Políticas
2. Definições
3. Arcabouço Legal
4. Descrição do serviço
5. Direitos do usuário
6. Responsabilidades do usuário e da administradora
7. Mudanças no Termo de Uso
8. Informações para contato
9. Foro

H. O Encarregado

Recomenda-se que o encarregado, na etapa de Construção/Execução, realize as atividades apresentadas a seguir:

1. Implementação das ações identificadas na fase de Iniciação e Planejamento;

2. Demonstração, para os dirigentes da administradora, do progresso e dos resultados obtidos com as atividades envolvendo o inventário dos dados e a divulgação e conscientização da LGPD junto aos colaboradores.

3. Se necessário, redefinição de prioridades, baseando-se nos resultados alcançados e no retorno dos dirigentes e colaboradores da administradora.

4. Estabelecimento e manutenção de documentação relacionado à LGPD e aos dados pessoais tratados na administradora, com informações sobre: atividades em andamento e planejadas; responsáveis pelos serviços e sistemas que utilizam dados pessoais; e incidentes e vazamento de dados pessoais.

5. Definição de mecanismos de reportes internos, assegurando transparência e rapidez na troca de informação, além de reafirmar o papel como facilitador, suporte e nunca como obstáculo.

8. Plano de Execução do PGP nas Administradoras

Considerando que as administradoras serão Controladoras e Operadoras, ***dependendo de condições especificas na execução dos serviços contratados com seus clientes***, é de suma importância que seja confeccionado um Programa de Governança em Privacidade - PGP, considerando as condições da prestação de serviço acordadas e delimitadas pela administradora a seus clientes. De qualquer forma haverá a necessidade de acompanhamento e orientação a seus clientes (Condomínio, Proprietários e Locatários).

Conforme definido o ***PGP das administradoras deve incluir estratégias, habilidades pessoais, processos e ferramentas que precisam conquistar a confiança dos condomínios e associações, ao mesmo tempo, cumprindo as exigências apresentadas nas normativas da LGPD***, além de orientar seus clientes quando estes forem os operadores dos dados, considerando administração de condomínios e locação de imóveis.

Considerando estes fatores, o primeiro passo para confecção do PGP é a alta direção da administradora nomear o Encarregado – DPO, que juntamente com a alta direção definirá o comitê LGPD (Comitê de Governança Digital) e estes conduzirão a execução do programa. O entendimento da empresa para a importância do PGP e o papel do DPO é fundamental para o sucesso do projeto, sendo assim é altamente recomendado que seja realizada uma reunião com todos os gestores (1º nível e níveis intermediários) de forma a promover o entendimento do projeto e disseminação a todos os colaboradores e parceiros de negócio.

É fundamental que o comitê LGPD, formado por diretores, gestores e gerentes propaguem a ideia de que a LGPD seja estudada e compreendida internamente por todos os colaboradores da administradora, de forma a garantir o comprometimento de todos no projeto. A partir desta reunião será elaborado o cronograma do projeto, agendamento de reuniões de acompanhamento, plano estratégico de comunicação e campanha para engajamento dos colaboradores nas próximas etapas do programa – Papeis e responsabilidades definidos.

PERGUNTAS GERAIS

O que é Dado Pessoal?

Dado pessoal é toda e qualquer informação relacionada a uma pessoa física identificada ou que possa ser identificada, como por exemplo: nome, CPF, RG, data de nascimento, endereço, e-mail, telefone, dados bancários, geolocalização, entre outros. Ou seja, é toda informação vinculada a pessoa natural, de forma direta ou indireta.

Exemplos:

- Nome,
- Números de documentos (RG, CPF, carteira de trabalhos, etc);
- Endereço;
- Data de nascimento;
- Fotos;
- Número de telefone ou celular;
- E-mail;
- Perfil do Facebook, Instagram, LinkedIn e outras redes sociais;

O que é tratamento de dados?

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.

Além desses, também são considerados pessoais, mesmo que indiretamente, os seguintes dados:

- Histórico de compras em determinado site;
- Dados referentes à localização;
- Biometria e reconhecimento facial, etc.

Quais são os dados pessoais sensíveis?

São considerados sensíveis os dados pessoais 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.

Quem é o titular do dado?

É a pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento. Exemplo: Locador, locatário, condômino.

Alguns exemplos de situações em que o tratamento de dados é autorizado pela Lei:

- **Contrato -** Nos procedimentos preparatórios e antes de assinar o contrato, bem como para que o contrato consiga ser cumprido;
- **Interesse legítimo do controlador ou de terceiros;**
- **Consentimento -** Quando o titular de dados dá a sua permissão ao controlador para que trate de seus dados pessoais;
- **Exercício regular de direitos em processo judicial, administrativo ou arbitral;**
- **Proteção da vida ou integridade física do titular ou de terceiros;**
- **Proteção de crédito.**

Quais são os direitos dos titulares dos dados?

Conforme previsto na LGPD, o titular de dados pessoais possui uma série de direitos perante o controlador, tais como:

- Acesso aos dados;
- Informação sobre com quem seus dados são compartilhados;
- Informação sobre quem realiza o tratamento, bem como suas informações de contato;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação dados desnecessários, excessivos ou tratados de maneira inadequada, entre outros.

Por qual finalidade a administradora realiza o tratamento de dados?

Basicamente por três finalidades, sendo elas: Atender questões contratuais onde a admistradora necessita de dados dos clientes para emissão de boletos (por exemplo). Atender a questões legais, quando documentos são guardados mesmo após o fim do contrato. Registro de funcionário de condomínio (por exemplo). Auxiliar na prospecção de novos clientes, quando coletamos dados para futuro contato (por exemplo).

A LGPD é aplicável a todos os negócios da administradora?

Sim, a LGPD é aplicável a todos os setores de controle de dados pessoais internos e externos de clientes, logo todos os negócios são impactados pela Lei 13.709. São exemplos:

- Administração;
- Locação;
- Compra e venda.

Quais cuidados que devem ser observados pelos colaboradores quando do tratamento de dados pessoais?

O colaborador é responsável pela proteção e segurança dos dados pessoais aos quais tiver acesso, quando realizar a coleta, utilização, processamento, compartilhamento.

Destacando que **dado pessoal**, para este efeito, é qualquer informação relativa uma pessoa física que esteja identificada ou que possa ser identificada, tais como:

- Nome,
- Números de documentos (RG, CPF, carteira de trabalhos, etc);
- Endereço;
- Data de nascimento;
- Fotos;
- Número de telefone ou celular;
- E-mail;
- Perfil do Facebook, Instagram, Linkedin e demais redes sociais;

Essa definição também inclui hipóteses não tão óbvias, como identificadores digitais (por exemplo, o endereço de IP do seu smartphone ou cookies instalados no navegador que você utiliza para acessar a internet), dados referentes à sua localização, seus dados bancários, seu histórico de compras em determinado site, entre muitos outros.

Para assegurar tal conformidade, recomendamos alguns documentos que a administradora deverá possuir para que auxiliar na orientação de todo o seru corpo de colaboradores:

- **Política de Segurança Tecnológica**
- **Política de Acessos**
- **Código de Ética e Conduta**

O colaborador deverá obedecer às normas e políticas da empresa a respeito do uso e proteção de dados pessoais e segurança de informação, não podendo, de forma alguma, fazer qualquer uso não autorizado desses dados e informações, sendo proibido, em especial:

a) coletar, utilizar, processar, armazenar, excluir ou realizar qualquer outro tratamento de dados pessoais desnecessários às suas funções ou em desacordo com tais normas e políticas, como, por exemplo, o envio de dados pessoais para e-mails e drives particulares ou sua guarda em mídias e equipamentos não autorizados; e

b) copiar, fotografar, gravar ou reproduzir, bem como compartilhar ou divulgar original ou cópia, inclusive documentos, telas, mídias ou arquivos, entre outros, como, por exemplo a postagens de imagens ou vídeos em redes sociais ou seu envio para pessoas externas à empresa.

Demais cuidados que deverão ser observados durante a rotina de trabalho:

• Não deixar documentos diversos expostos na mesa ou em gaveta sem a chave. O mesmo vale para pen drive ou hd externo
• Bloquear sempre a tela do equipamento quando deixar a estação de trabalho;(notebook, tablet, smartfone)
• Confirmar para qual impressora está enviando o documento antes de imprimi-lo
• Confirmar para qual e-mail está digitalizando o documento antes de digitalizar.
• Coletar todos os documentos enviados/digitalizados/copiados nas impressoras
• Em caso de uso ou reprodução de documentos fora da empresa, ficar atento para que nenhum documento se perca ou seja manuseado por pessoa indevida.
• Não compartilhar nenhuma senha de acesso;
• Descartar com segurança (eliminar toda possibilidade de leitura do documento) qualquer tipo de rascunho/anotação que possa identificar o cliente, ex-cliente, funcionário, ex-funcionário, prestador de serviço ou ex-prestador de serviço
• Conversas presenciais, remotas ou por áudio, que exponham dados pessoais, devem ser evitadas
• Troca de informações, que exponham dados pessoais, por meios digitais (whatsapp, e-mail, redes sociais) devem ser evitadas

Caso o titular do dado solicite o acesso às informações sobre o tratamento de seus dados, o que deve ser feito?

Deve haver formalização do pedido e este ser encaminhado formalmente à administradora, por carta ou e-mail, onde a solicitação será analisada e respondida para o cliente. De imediato, o funcionário da administradora deverá retornar ao cliente citando que sua solicitação será respondida pelo departamento responsável, dependendo este do tipo de tratamento de dado que estiver realizando.

Posso ofertar a meus clientes outros produtos da minha empresa?

Sim, desde que estejam ligados à prestação de serviço original. Caso não sejam, será necessário solicitar o consentimento para a oferta.

Posso fazer parcerias com empresas para vender produtos para a minha base?

Não, a Lei Geral de Proteção de Dados foi elaborada justamente para proteger os dados das pessoas naturais. Nenhuma venda de informações é permitida. Ofertas de outros fornecedores só poderão ser realizadas com o consentimento de nossos clientes.

Quais são os cuidados que tenho que ter na comunicação?

Vários cuidados são necessários na comunicação com os clientes, porém os principais cuidados estão contidos em dois princípios da lei 13.709, que são:

Princípio da Finalidade: A comunicação baseada na finalidade da lei precisa apresentar os propósitos legítimos, ser específica e explícita.

Princípio da Transparência: A comunicação baseada na transparência que a lei preza, deve ser clara, objetiva e apresentar fácil entendimento ao público.

O cliente pode se excluir da base?

Não, ele não tem acesso a base da empresa e nem deve ter autonomia para isso.

No geral, o cliente pode pedir exclusão do cadastro da administradora? Se não, porquê?

O cliente tem o direito de pedir a exclusão, porém a empresa precisa atender a três passos fundamentais antes de realizar o atendimento ao descarte ou a anonimização dos dados, são eles:

- Finalidade primária e secundária
- Bases legais obrigatórias
- Prazo prescricional

Prospects inativos podem ser excluídos por não manter relação com a administradora

Enquanto cliente ativo, não poderá ser atendida a exclusão pois possui relacionamento vigente, salvo aqueles que não estão ligados diretamente à prestação do serviço. Caso seja demandado, devemos apresentar os dados que possuímos dos clientes e ex-clientes.

LEITURAS RECOMENDADAS

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
https://www.gov.br/anpd/pt-br

	ADMINISTRADORA			CONDOMÍNIO		
DEPARTAMENTO PESSOAL	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
ADMISSÃO	X	X	A Administradora deverá coletar somente os dados necessários, informando ao colaborador a finalidade da coleta de tais dados e fica a partir desse momento responsável pelos mesmos, não podendo compartilhar com outras pessoas ou empresas.	X	X	As informações são fornecidas pelo condomínio e o colaborador encaminhado à Administradora pelo próprio condomínio, sendo eles os responsáveis pelos dados cedidos para a admissão
DEMISSÃO	X	X	A Administradora deve reter apenas os dados que a lei exige. Eliminar dos sistemas e documentos (físico e digital) de forma a evitar possíveis vazamentos	X	X	As informações são fornecidas pelo condomínio e o colaborador encaminhado à Administradora pelo próprio condomínio, sendo eles os responsáveis pelos dados cedidos para a demissão
BENEFÍCIOS	X	X	A Administradora deverá se certificar que no contrato que possui com as empresas parceiras consta cláusula de confidencialidade que respeite e cumpra a lei 13.709 LGPD, impedindo o compartilhamento de dados com outras pessoas ou empresas	X	X	O condomínio deverá se certificar que a sua Administradora cumpre a lei 13.709 LGPD, impedindo de compartilhar os dados de seus condôminos com outras pessoas ou empresas que estão fora da prestação de serviço pactuada entre as partes
FÉRIAS	X	X	A Administradora deverá coletar e armazenar somente os dados necessários, informando ao colaborador a finalidade da coleta de tais dados e fica a partir desse momento responsável pelos mesmos, não podendo compartilhar com outras pessoas ou empresas.	X	X	As informações são fornecidas pelo condomínio que assume os riscos das informações cedidas a Administradora
	ADMINISTRADORA			**CONDOMÍNIO**		
CONTAS A PAGAR	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
RECEPÇÃO DE CONTAS A PAGAR	X	X	A Administradora é responsável pelos dados coletados. Proibida de compartilhar os dados e responsável pelo vazamento, tendo ocorrido por seus colaboradores ou mesmo se ocorrer através do banco.	X	X	As informações são fornecidas pelo condomínio que assume os riscos das informações
ENVIO AO BANCO DAS CONTAS A PAGAR	X	X	A Administradora é responsável pelos dados enviados ao banco. Proibida de compartilhar os dados e responsável pelo vazamento, tendo ocorrido por seus colaboradores ou mesmo se ocorrer através do banco.	X	-	O condomínio segue responsável pelos dados enviados a Administradora que enviou ao banco para pagamento Existem casos que o condomínio não informa os dados, então a Administradora é quem busca as informações com o fornecedor
RETORNO BANCÁRIO DO PAGAMENTO	X	X	A Administradora é responsável pelo retorno dos dados pelo banco. Proibida de compartilhar os dados e responsável pelo vazamento, tendo ocorrido por seus colaboradores ou mesmo se ocorrer através do banco.	X	-	O condomínio segue responsável pelos valores recebidos pela Administradora
CONCILIAÇÃO DE PAGAMENTO	X	X	A Administradora é responsável pelos dados recebidos e conciliados. Proibida de compartilhar os dados e responsável pelo vazamento.	X	-	O condomínio ratifica as informações sempre que acata a pasta de prestação de contas, assumindo a responsabilidade pelos dados
	ADMINISTRADORA			**CONDOMÍNIO**		
CONTAS A RECEBER	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
RECEBIMENTO DE VALORES	X	X	A Administradora é responsável pelos dados recebidos e conciliados. Proibida de compartilhar os dados e responsável pelo vazamento.	X	-	O condomínio possui a responsabilidade pelos valores enviados a Administradora, apesar de não ser o operador da atividade

	ADMINISTRADORA			CONDOMÍNIO		
CONTAS A RECEBER	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
CONCILIAÇÃO DE VALORES RECEBIDOS	X	X	A Administradora é responsável pelos dados recebidos e conciliados. Proibida de compartilhar os dados e responsável pelo vazamento.	X	-	O condomínio possui a responsabilidade pelos valores enviados a Administradora, apesar de não ser o operador da atividade
	ADMINISTRADORA			**CONDOMÍNIO**		
COBRANÇA	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
ENVIO DE COBRANÇA	X	X	A Administradora deverá se certificar que no contrato que possui com as empresas parceiras consta cláusula de confidencialidade que respeite e cumpra a lei 13.709 LGPD, impedindo o compartilhamento de dados com outras pessoas ou empresas	X	-	O condomínio possui responsabilidade sobre os documentos de cobrança recebidos da Administradora, sendo proibido de violar, descartar, extraviar e distribuir de forma equivocada
IDENTIFICAÇÃO DE INADIMPLENTE	X	X	A Administradora é responsável pelos dados recebidos. Proibida de compartilhar os dados e responsável pelo vazamento.	X	X	O condomínio é responsável pelos dados enviados. Proibida de compartilhar os dados e responsável pelo vazamento.
	ADMINISTRADORA			**CONDOMÍNIO**		
EXPEDIÇÃO	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
ENVIO DE DOCUMENTAÇÃO PELA ADM	X	X	A Administradora é responsável pela documentação que envia ao condomínio, sendo ela responsável por qualquer vazamento de dados ocorridos até o recebimento pelo condomínio.	X	-	O condomínio é responsável por receber e cuidar para que os documentos recebidos não sejam vazados
RECEBIMENTO DE DOCUMENTAÇÃO PELA ADM	-	X	A Administradora é responsável por receber e cuidar para que os documentos recebidos não sejam vazados	X	X	O condomínio é responsável pela documentação que envia a Administradora, sendo ele responsável por qualquer vazamento de dados ocorridos até o recebimento pela Administradora.
	ADMINISTRADORA			**CONDOMÍNIO**		
ATENDIMENTO AO CLIENTE	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
ATENDIMENTO REMOTO	X	X	É obrigação da Administradora a certificação de que está trocando informações com seu cliente, através de confirmações.	X	X	É obrigação do condômino a certificação de que está trocando informações com sua Administradora, através de confirmações.
ATENDIMENTO FÍSICO	X	X	A Administradora precisa informar a finalidade de todos os dados coletados.	X	X	É de liberalidade do titular dos dados fornecedor ou não de seus dados para o atendimento, podendo impedi-lo de receber o que deseja.
ALTERAÇÃO CADASTRAL	X	X	A Administradora precisa solicitar dados e certidões para a alteração dos dados de seus clientes, devendo na sequência armazená-los em local sem acesso múltiplo e fica proibida de compartilhar os mesmos com outras pessoas ou empresas.	X	-	O condômino precisa se certificar que só está fornecendo o necessário para a alteração cadastral.

	ADMINISTRADORA			CONDOMÍNIO		
MARKETING	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
EMAIL MARKETING	X	X	A Administradora não pode em qualquer hipótese fornecer dados de seus clientes para outras empresas ou pessoas. Somente pode ofertar serviços diretamente ligados à sua operação, devendo sempre ter a opção de não mais receber tais informes.	-	-	O condômino precisa se atentar para não cair em fraudes eletrônicas, e assim passar informações indevidas, proporcionando o vazamento de informações (recomendação)
ENVIO DE SMS	X	X	A Administradora não pode em qualquer hipótese fornecer dados de seus clientes para outras empresas ou pessoas. Somente pode ofertar serviços diretamente ligados a sua operação, devendo sempre ter a opção de não mais receber tais informes.	-	-	O condômino precisa se atentar para não cair em fraudes eletrônicas, e assim passar informações indevidas, proporcionando o vazamento de informações (recomendação)
MALA DIRETA	X	X	A Administradora não pode em qualquer hipótese fornecer dados de seus clientes para outras empresas ou pessoas. Somente pode ofertar serviços diretamente ligados a sua operação, devendo sempre ter a opção de não mais receber tais informes.	-	-	O condômino precisa se atentar para não cair em fraudes eletrônicas, e assim passar informações indevidas, proporcionando o vazamento de informações (recomendação)
MARKETING DIGITAL	X	X	A Administradora não pode em qualquer hipótese fornecer dados de seus clientes para outras empresas ou pessoas. Somente pode ofertar serviços diretamente ligados a sua operação, devendo sempre ter a opção de não mais receber tais informes.	-	-	O condômino precisa se atentar para não cair em fraudes eletrônicas, e assim passar informações indevidas, proporcionando o vazamento de informações (recomendação)
	ADMINISTRADORA			CONDOMÍNIO		
CAPTAÇÃO	CONTROLADOR	OPERADOR	CUIDADOS	CONTROLADOR	OPERADOR	CUIDADOS
CAPTAÇÃO RECEPTIVA	-	X	A Administradora deve ter todo o cuidado com o recebimento e tratamento das informações deste prospect	X	X	Neste momento em que o síndico /condômino procura a Administradora para receber uma proposta, o síndico é controlador e operador dos dados, não tendo a Administradora nenhuma responsabilidade.
CAPTAÇÃO PROATIVA	X	X	Nesta atividade de captação de clientes no formato proativo, a Administradora assume a responsabilidade pelos dados que está recebendo. A informação de nome e telefone do síndico/condômino deve respeitar a liberalidade de uso.	-	-	O condômino precisa se atentar para não cair em fraudes eletrônicas, e assim passar informações indevidas, proporcionando o vazamento de informações (recomendação)
IMPLANTAÇÃO DE CLIENTES	X	X	A Administradora ao receber os dados, seja de clientes ou mesmo de outra Administradora através de portabilidade, é responsável pelos dados, sendo proibida de partilhar ou mesmo divulgar os mesmos	X	-	O condomínio é corresponsável pelos dados enviados a Administradora para a implantação do condomínio e deve ratificar os dados sempre que oportuno, caso necessite de alguma correção é seu direito o pedido a Administradora
SORTEIOS	X	X	A Administradora se torna responsável pelos dados quando os recebe e não deve compartilhar com outras empresas. A coleta de dados deve respeitar o princípio da necessidade, não coletando dados além do que será preciso para o sorteio/contato. Sinalizar que os dados coletados servirão para contato futuro, e que em tempo serão devidamente descartados, de forma a evitar possíveis vazamentos	-	X	É de liberalidade do titular dos dados fornecedor ou não seus dados para o sorteio
E-MAIL MKT	X	X	A Administradora poderá enviar e-mails de marketing somente quando diz respeito a sua própria prestação de serviço, ficando proibida a dividir os dados com outras empresas. Sinalizar que os dados coletados servirão para contato futuro, e que em tempo serão devidamente descartados, de forma a evitar possíveis vazamentos	-	-	O condomínio/condômino pode ter a opção de não querer mais receber o e-mail e pedir descadastramento

Manual Operacional da LGPD

PARA ADMINISTRADORAS DE CONDOMÍNIOS E IMÓVEIS

Lei nº 13.709/2018

Versão 1.0