

GUIA LGPD

INCORPORAÇÃO, INTERMEDIACÃO
E ADMINISTRAÇÃO DE IMÓVEIS
E CONDOMÍNIOS



FICHA TÉCNICA

Presidente

Basilio Chedid Jafet

Curadoria

Moira Regina de Toledo Bossolani

Coordenação geral

Lisa Lima

Parceria

Equipe Consultiva Opice Blum
Advogados

Edição e Revisão

Assessoria de Comunicação do
Secovi-SP

Diagramação

DK Publi Estúdio Criativo

Secretaria

Eliana Araújo
Keila de Souza

Nosso especial agradecimento aos vice-presidentes:

Adriano Sartori – Gestão Patrimonial e Locação
Emilio Rached Esper Kallas – Incorporação e Terrenos Urbanos
Carlos Alberto de Moraes Borges – Tecnologia e Sustentabilidade

Claudio Kawa Hermolin – Intermediação Imobiliária e Marketing

Agradecimentos

Carlos Pinto Del Mar
Eric Keller Tavares de Camargo
Guido Cussioli Neto
Jaques Bushatsky
Kelma Camargo
Nelson Parisi Jr.
Olivar Vitale Jr.
Rodrigo Abrahão
Sergio Meira de Castro Neto
Tácito Monteiro

Secovi-SP

Ingrid Ferreira
Karina Zuanazi Negreli
Maria do Carmo Gregório
Patrícia Machado Bittencourt
Rosana Souza Pinto

Contato Secovi-SP: (11) 5591-1300

Fale conosco: secovi@secovi.com.br

PREFÁCIO

O objetivo deste documento é apresentar às empresas do setor imobiliário representadas pelo Secovi-SP, um guia sobre aspectos relacionados à LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) que afetam as atividades de incorporação imobiliária, vendas e locação de imóveis, bem como administração de condomínios, indicando os principais pontos de conexão entre esses players do mercado.

A linguagem acessível e objetiva foi utilizada buscando auxiliar na compreensão do processo de adequação, ampliando o alcance dos conceitos básicos sobre a legislação, além de citar situações práticas presentes na rotina das empresas.

SUMÁRIO

INTRODUÇÃO: SECOVI-SP E A IMPORTÂNCIA DA LGPD NO ÂMBITO DE SUA ATUAÇÃO.....	12
--	-----------

CAPÍTULO I - PRINCIPAIS CONCEITOS DA LGPD	15
--	-----------

Que tipo de informação é considerada como dado pessoal?	16
---	----

O que são dados pessoais sensíveis?.....	16
--	----

Quais atividades são consideradas tratamento de dados pessoais?	17
---	----

A quem se aplica a LGPD? Ela se aplica apenas para o tratamento de dados realizados online ou virtualmente?	18
---	----

Quem é o titular dos dados pessoais? Quais são seus direitos?	18
---	----

Quais os principais atores na LGPD?	20
---	----

Como identificar quem é controlador e quem é operador?	21
--	----

Princípios e bases legais: como realizar o tratamento de dados pessoais em conformidade com a LGPD? Preciso sempre pedir a autorização do titular de dados?	24
---	----

Quais são as penalidades previstas na LGPD?	29
---	----

CAPÍTULO II - ATIVIDADES MAIS COMUNS DE TRATAMENTO DE DADOS NO MERCADO IMOBILIÁRIO	30
---	-----------

A. Tratamento de dados de colaboradores.....	31
---	-----------

Agora que a LGPD está em vigor, o que muda no tratamento dos dados dos colaboradores pela empresa? 31

Qual a importância de um termo de confidencialidade?..... 32

O que são políticas de segurança da informação e qual a sua importância?..... 33

B. Tratamento de dados de clientes 34

Como a empresa deve se preparar para lidar com dados de clientes? 34

A LGPD autoriza o compartilhamento de dados dos clientes de uma empresa com parceiros comerciais? 35

Se a empresa é a controladora dos dados dos clientes, isso significa que os colaboradores são operadores?..... 35

C. Relação com titulares de dados e com a ANPD 36

A contratação de um Encarregado (DPO) é obrigatória? Como proceder? 36

Como agir diante de requisições de titulares de dados? É necessário ter um canal específico para esta finalidade? 37

D. Contratação de fornecedores e prestadores de serviço 37

Os fornecedores e prestadores de serviço precisam estar adequados à LGPD?..... 37

Que cuidados são necessários ao contratar produtos como softwares e sistemas? 38

E. Segurança: controle de acesso..... 38

Quais cuidados devem ser tomados com o controle de acesso ao edifício via cartão ou crachá? 38

O que é importante saber sobre monitoramento por câmeras? 39

CAPÍTULO III - A ATIVIDADE DE INCORPORAÇÃO 40

A. Regularização da incorporação 41

Que cuidados a incorporadora deve ter ao lidar com os documentos necessários para regularizar a incorporação? 41

Uma vez regularizada a incorporação e as vendas estejam prontas para iniciar, quais cuidados a incorporadora deve ter ao procurar potenciais compradores? Com quem os dados podem ser compartilhados? 41

Que cuidados a incorporadora deve ter em se tratando da assembleia de instalação do condomínio que ocupará o empreendimento? 41

Uma vez que o condomínio esteja instalado e operando normalmente, a incorporadora ainda possui algum dever de compartilhar dados com o síndico ou outros envolvidos com o condomínio? 42

B. Vendas e atuação de corretores associados 42

Quais cuidados devem ser adotados nos estandes de vendas de empreendimentos imobiliários? 42

Para a divulgação on-line de empreendimentos, quais os principais cuidados que devem ser tomados? 44

No caso de corretores associados que trabalham com bases de dados próprias, que cuidados tomar para garantir que o tratamento de dados está em conformidade com a LGPD? 45

C. Outros casos de compartilhamento de dados 46

Até que ponto os dados de clientes podem ser compartilhados com parceiros comerciais da incorporadora? 46

Em casos de fiscalização da execução das obras, é permitido compartilhar os dados dos colaboradores e prestadores de serviço envolvidos quando solicitado? 47

Se um cliente adquiriu um produto imobiliário diretamente com outra empresa, mas a incorporadora está envolvida na execução do projeto, é possível compartilhar os dados desse cliente? 47

CAPÍTULO IV - A ATIVIDADE DE INTERMEDIACÃO DE VENDAS E LOCAÇÃO 48

A. Prospecção de clientes e bases de dados 49

A LGPD autoriza a prospecção de clientes? Quais são as limitações? 49

É possível utilizar os dados de um cliente para informá-lo de outros empreendimentos futuros? 50

É possível filtrar os titulares por determinados atributos (como renda) sem que isso configure como discriminação? 50

Há algum cuidado especial com dados disponíveis publicamente? Eles podem ser utilizados para fins de prospecção de clientes? 51

Campanhas de Indicação: como organizá-las em conformidade com a LGPD? 51

B. Diligências do corretor 52

A LGPD permite a verificação de dados do comprador do imóvel? Como justificar o tratamento desses dados? 52

O corretor pode receber os documentos necessários para fechar o negócio em seu número particular de WhatsApp (ou serviço de mensageria equivalente)? 53

CAPÍTULO V - ADMINISTRAÇÃO DE LOCAÇÃO 54

A. Avaliação de risco do locatário 55

Quais cuidados são necessários com os documentos do candidato a locatário? 55

Caso o perfil do candidato a locatário seja recusado, devo informar a ele os motivos da recusa? 55

B. No decorrer do contrato 56

Quais cuidados são necessários nos momentos de entrega das chaves? É permitido verificar a identidade de quem as está retirando? 56

É correto utilizar redes sociais e/ou aplicativos de mensageria para realizar comunicados importantes sobre a administração da locação? 56

Em caso de cobranças e ações judiciais, como lidar com os dados pessoais dos envolvidos? 57

C. Contratação de terceiros 58

Que cuidados são necessários com a contratação de concessionárias e prestadores de serviços? 58

Quais cuidados devem ser tomados ao contratar terceiros para a execução de obras?	58
---	----

CAPÍTULO VI - ADMINISTRAÇÃO DE CONDOMÍNIOS..... 59

A. Gerenciamento de dados de condôminos..... 60

A LGPD permite compartilhar dados de condôminos?	60
--	----

No portal eletrônico da administradora, quem deve ter acesso aos dados pessoais dos condôminos?	60
---	----

Como lidar com as questões relacionadas à inadimplência de condôminos?	61
--	----

Se o condomínio utiliza o formato digital para disponibilizar as pastas de prestação de contas, que dados podem ser exibidos e quais devem ser preservados?	61
---	----

Sobre os grupos de condôminos em aplicativos de mensageria (como WhatsApp): que informações podem ser compartilhadas? Qual a responsabilidade do síndico e/ou do administrador pelo que é falado ali?	61
---	----

B. Assembleia de condôminos..... 62

Nas ocasiões em que a assembleia de condôminos é gravada, as imagens podem ser compartilhadas a pedido de um condômino?	62
---	----

A lista de presença da assembleia necessita ser registrada juntamente com a ata?	63
--	----

É possível minimizar os dados constantes na lista de presença da assembleia?	64
--	----

Nos casos de procuração de assembleias, quais dados precisam ser informados e constar do documento? Podem fornecer cópia da procuração quando solicitado?	64
---	----

C. Segurança.....65

Para atividades voltadas à segurança, como sistema de vigilância e portaria, é permitido compartilhar os dados pessoais dos condôminos com empresas terceirizadas? 65

O que é importante saber sobre o monitoramento por câmeras nos condomínios? 65

O que fazer com o registro de visitantes que circulam nos condomínios, especialmente comerciais? Quais dados devem ser solicitados? 66

Que cuidados devem ser tomados caso o condomínio adote portaria eletrônica? ... 67

Existem medidas especiais para o tratamento de imagens de crianças e adolescentes? 68

Que cuidados devem ser tomados com o Livro de Registro de Ocorrências? 69

D. Relação entre o condomínio e a administradora 70

Quando se fala na proteção de dados dos condôminos, quem é o responsável por eles: o síndico ou a administradora do condomínio? 70

Como proceder com os dados pessoais dos condôminos e moradores se o contrato com a administradora for rescindido? 71

E. Cuidados sanitários..... 71

Em caso de epidemias ou surtos de doenças infectocontagiosas no condomínio, que cuidados devem ser adotados com a informação aos condôminos e o tratamento de seus dados pessoais? 71

CAPÍTULO VII - COMPARTILHAMENTO DE DADOS E RELAÇÃO ENTRE OS PLAYERS DO MERCADO IMOBILIÁRIO 73

A. Preparando o terreno: bases legais e a expectativa do titular de dados..... 74

B. Compartilhamentos necessários no decorrer dos negócios..... 75

Transferências de administradoras de condomínio..... 75

Compartilhamento de documentos e outros dados obrigatórios para regularização do ativo imobiliário 76

Compartilhamento de dados entre incorporadora e empresa responsável pelo lançamento do empreendimento 76

CAPÍTULO VIII - O PROCESSO DE ADEQUAÇÃO À LGPD NA PRÁTICA 78

A. Medidas do Plano de Ação 79

Registro e mapeamento dos dados 79

Nomeação de um Encarregado pela Proteção de Dados Pessoais (DPO) 80

Criar políticas e procedimentos..... 80

Divulgar normas, políticas e procedimentos e realizar treinamentos 81

Criar canal de comunicação com o titular e divulgá-lo amplamente 81

Revisar e aditar contratos 81



INTRODUÇÃO:

SECOVI-SP E A IMPORTÂNCIA DA LGPD NO ÂMBITO DE SUA ATUAÇÃO



O Secovi-SP faz história desde 1946, cumprindo o seu compromisso com o Estado de São Paulo por meio do desenvolvimento do setor urbano ao lado de parceiros públicos, corporativos e da grande mídia.

Hoje, mais de 90 mil empresas são representadas pelo Secovi-SP. Um resultado alcançado com trabalho e muita dedicação. Suas atuações se dão por intermédio de vice-presidências e diretorias nas áreas de incorporação, loteamentos, comercialização, administração imobiliária e condomínios, tecnologia, sustentabilidade, interior e shopping centers. Vem, ainda, se dedicando ao grupo de Empreendedorismo e Inovação (NE), voltado à formação daqueles que vão responder pelo futuro das atividades no setor, à fomentar novas iniciativas fazendo a conexão destas com o “mercado tradicional” proporcionando assim um hub de inovação.

Além da forte ação institucional, o Secovi-SP elabora e dissemina conteúdo e informações relevantes entre as empresas do mercado imobiliário, como pesquisas, índices e legislações. É neste contexto que busca propiciar aos seus representados o aprofundamento do conhecimento na Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais, que chamaremos de “LGPD”.

Apesar de ser uma lei muito recente, em vigor a partir de setembro de 2020, a LGPD representa uma grande mudança no modo como os dados pessoais são tratados no Brasil. Por um lado, ela estabelece os direitos dos titulares sobre os seus dados pessoais e as informações que lhes dizem respeito. Por outro lado, ela também serve de mapa para que os *players* do mercado que atuam no tratamento de dados possam navegar por um labirinto complexo e, até pouco tempo atrás, sem regras claras.

No âmbito de atuação do Secovi-SP, dados pessoais são necessários em diversas situações, especialmente porque há muitos compartilhamentos entre os agentes envolvidos no surgimento e gerenciamento do ativo imobiliário — desde a incorporação do imóvel à sua construção e venda das unidades, até o gerenciamento do dia a dia dos dados de colaboradores, condôminos, potenciais compradores, entre tantos outros. Ao mesmo tempo que é essencial para o mercado, este tratamento deve ser realizado de maneira correta e segura, respeitando os direitos dos indivíduos a quem se referem essas informações.

Com este cenário em mente, o **Secovi-SP**, em parceria com o escritório **Opice Blum, Bruno e Vainzof Advogados Associados**, apresenta ao leitor este guia, com relevantes informações sobre a LGPD e respondendo às principais dúvidas sobre como a lei afeta o dia a dia das empresas do setor imobiliário.

Lembramos que este guia é dinâmico, pois novas normas e diretrizes surgem todos os dias. Por isso, em caso de dúvidas, entre em contato conosco.



CAPÍTULO I

PRINCIPAIS CONCEITOS DA LGPD



Que tipo de informação é considerada como dado pessoal?

A LGPD define como dado pessoal **toda e qualquer informação que identifique ou possa identificar um indivíduo**. Exemplos clássicos de dados pessoais são:

- dados cadastrais: nome, endereço, data de nascimento, números de documentos de identificação, número de telefone, e-mail etc.;
- dados bancários: número da conta, senha, dados de cartão de crédito ou débito etc.;
- dados de navegação na internet: endereço de IP, cookies, tipo de dispositivo, data e hora do acesso, histórico de navegação etc.;
- dados de localização (obtidos pelo GPS do seu celular, por exemplo);
- dados de saúde: seu peso, doenças preexistentes, condições de saúde no geral; e
- dados biométricos: sua impressão digital, sua biometria facial etc.

Em resumo:

Tudo depende do contexto: se for possível determinar a identidade do indivíduo — direta ou indiretamente — por meio daquela informação ou de um conjunto de informações, então estamos falando de dados pessoais.

O que são dados pessoais sensíveis?

Os dados sensíveis são uma **categoria especial** de dados pessoais que abrange:

- dados sobre a origem étnica ou racial do titular;
- dados sobre suas crenças religiosas ou opiniões políticas e filosóficas;

- dados sobre filiação a sindicato ou organização política, filosófica ou religiosa;
- dados sobre a saúde e vida sexual; e
- dados genéticos ou biométricos.

Classificados como categoria especial na LGPD, merecem cuidados especiais de tratamento e política de segurança da informação, pois, se mal utilizados, podem provocar **discriminação contra o titular**.

Quais atividades são consideradas tratamento de dados pessoais?

Tratamento de dados é o nome amplo utilizado pela LGPD para se referir a toda e qualquer atividade realizada com dados pessoais. O tratamento envolve ações das mais diversas, incluindo **coletar, armazenar, produzir, classificar, acessar, reproduzir, transmitir, distribuir, arquivar, analisar, modificar, transferir, eliminar** e muitas outras. No cotidiano das atividades relacionadas às empresas imobiliárias, há tratamento de dados em uma série de atividades, como, por exemplo:

- registros e atividades relacionadas às assembleias dos condôminos;
- coleta dos dados do adquirente de um determinado imóvel, para celebrar o contrato de compra e venda com ele;
- negociação de contratos com prestadores de serviços das mais diversas áreas;
- envio de mala direta e e-mail marketing para clientes pessoa física; e
- gerenciamento dos dados dos colaboradores.

Vale ressaltar que estes são apenas alguns exemplos, dentre as várias atividades de tratamento realizadas pelas empresas imobiliárias em seus diversos ramos de atuação.

Para lembrar

- Qualquer atividade que envolva dados pessoais, desde a coleta até a sua de completa deleção, é considerada tratamento.

A quem se aplica a LGPD? Ela se aplica apenas para o tratamento de dados realizados on-line ou virtualmente?

A LGPD se aplica a **qualquer um que realize tratamento de dados pessoais** – tanto pessoas físicas quanto pessoas jurídicas.¹

A LGPD abrange o tratamento de dados pessoais em meios virtuais, mas também em meios físicos. Ou seja, as regras da lei não valem apenas para informações on-line ou em servidores, mas, também, para dados armazenados em arquivos físicos, fichas, livros de registros e todo e qualquer meio em que seja possível tratar os dados pessoais.

Quem é o titular dos dados pessoais? Quais são seus direitos?

O titular dos dados pessoais é o indivíduo que pode ser identificado a partir dos referidos dados. Como titular dos dados, o indivíduo tem uma série de direitos que lhe permitem, em certa medida, decidir como deseja que seus dados sejam tratados. O primeiro grupo de direitos diz respeito à **informação**, previsto no art. 9º da LGPD. É direito do titular obter, de maneira **clara e acessível**, informações sobre o tratamento de seus dados, incluindo:

- qual a finalidade específica para tal tratamento;
- como e por quanto tempo os dados serão tratados;

¹ As exceções para aplicação da LGPD são para tratamentos realizados:

- por pessoas físicas para fins particulares e não econômicos;
- para fins jornalísticos, artísticos ou acadêmicos;
- para fins de segurança pública e defesa.

- quem realiza o tratamento (ou seja, a identidade do **controlador**), bem como suas informações de contato;
- com quem seus dados são compartilhados e por que;
- quais as responsabilidades dos agentes envolvidos no tratamento de dados; e
- quais são e como exercer seus direitos em relação aos seus dados.

Via de regra, todas estas informações devem estar disponíveis na política ou aviso de privacidade do site ou aplicativo.

O segundo grupo de direitos relaciona-se com o **controle** do titular sobre os seus dados. O art. 18 da LGPD prevê que o titular pode, a qualquer momento, requisitar ao controlador dos dados:

- a confirmação se seus dados são tratados e ter acesso a eles;
- a correção dos dados incompletos, inexatos ou desatualizados;
- a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados de maneira inadequada;
- a portabilidade de seus dados para outro fornecedor de produto ou serviço; e
- a informação acerca das pessoas com quem o controlador compartilhou seus dados, incluindo entidades públicas e privadas.

Por fim, para os dados tratados com o **consentimento** do titular, a LGPD garante a ele o direito de solicitar ao controlador:

- a eliminação dos dados pessoais tratados com o seu consentimento;²
- a obtenção das informações sobre a possibilidade de não dar seu consentimento para determinado tratamento, e as consequências dessa negativa; e
- a revogação seu consentimento.

Para exercer esses direitos, o titular de dados deve entrar em contato com o controlador dos dados do produto ou serviço utilizado. É possível que a requisição do titular não possa ser atendida por motivos legais, quando, por exemplo, é necessário manter os dados pessoais por mais tempo, por determinação legal; ou técnico, quando, por exemplo, a solicitação não pode ser atendida por ausência de viabilidade técnica para tanto.

O atendimento do titular deve ocorrer sem custo para ele e dentro do prazo legal. A confirmação de existência ou o acesso aos dados pessoais deve ocorrer de forma imediata, se em formato simplificado. Caso a resposta ocorra de forma completa, ela poderá ocorrer em até 15 dias contados da data de requisição pelo titular.

Quais os principais atores na LGPD?

A LGPD menciona 4 atores principais: o **titular de dados**, os **agentes de tratamento** (controlador e operador), a Autoridade Nacional de Proteção de Dados – **ANPD** e o Encarregado ou **DPO**.

² As exceções para a eliminação dos dados são:

- se for necessário armazená-lo para cumprir uma obrigação legal ou regulatória
- se os dados foram utilizados para um estudo realizado por órgão de pesquisa
- se os dados foram transferidos para um terceiro
- se os dados foram anonimizados e mantidos para uso exclusivo do controlador

Principais Atores na LGPD	
Titular de Dados	A quem se referem os dados pessoais tratados.
Controlador	Quem tem o poder de tomar as decisões essenciais sobre o tratamento de dados.
Operador	Quem realiza o tratamento de dados conforme as decisões do controlador.
ANPD	Órgão da administração pública que será responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.
Encarregado	Pessoa indicada pelo controlador ou operador e que atuará como canal de comunicação entre o agente de tratamento para quem trabalha, os titulares e a ANPD.

Como identificar quem é controlador e quem é operador?

Este é um dos pontos mais importantes na definição das responsabilidades dos agentes envolvidos no tratamento de dados. Determinar quem é controlador e quem é operador não depende apenas de analisar as posições no contrato, mas, também, o modo como cada uma das partes irá tratar os dados pessoais e do seu poder de decisão sobre como este tratamento ocorrerá.

*Empresa ou condomínio tenderá a ser **controlador** quando...*

- **decide** coletar ou tratar dados pessoais
- **decide** a finalidade ou objetivo do tratamento
- **decide** quais dados coletar
- **decide** quais pessoas terão dados coletados
- obtém lucro, benefício ou **vantagem** comercial com o tratamento
- trata dados em razão de um **contrato com o titular**
- trata dados de seus **próprios colaboradores**
- toma **decisões** sobre os titulares com base no tratamento
- possui uma **relação direta** com o titular
- possui **total autonomia** sobre como lidar com os dados pessoais
- **nomeia terceiros (operadores)** para tratar dados em seu nome

*Empresa ou condomínio tenderá a ser **operador** quando...*

- **não decide** quais dados pessoais coletar
- segue **instruções de alguém** quanto ao tratamento de dados pessoais
- recebe os dados pessoais de **alguém que determina** o que deve fazer com eles
- **não decide** quando, como e de quem coleta dados pessoais
- **não decide** para qual finalidade ou objetivo os dados são tratados
- **não decide** quando ou com quem pode compartilhar dados
- **não decide** se mantém os dados, nem por quanto tempo mantê-los
- decide sobre a forma do tratamento, mas seguindo o **estabelecido em contrato** com alguém
- **não possui interesse direto** no resultado do tratamento dos dados

Princípios e bases legais: como realizar o tratamento de dados pessoais em conformidade com a LGPD? Preciso sempre pedir a autorização do titular de dados?

Para que o tratamento de dados seja feito em conformidade com a LGPD, é necessário seguir, no mínimo, dois requisitos:

- i. a adoção de uma **base legal** adequada; e
- ii. observar os **princípios legais** em qualquer etapa do tratamento dos dados pessoais.

Bases Legais

As chamadas **bases legais** são as hipóteses previstas na LGPD que autorizam o tratamento dos dados pessoais. Se uma atividade não se encaixar em uma dessas hipóteses, o tratamento não é autorizado pela LGPD. A seguir, listaremos as principais bases legais, destacando as mais utilizadas e adequadas às atividades realizadas pelo Secovi-SP e suas empresas representadas:

- **Consentimento.** Esta é uma das principais bases legais, e permite tratamento quando o titular de dados autoriza o controlador para que trate os seus dados pessoais. A LGPD impõe alguns requisitos para a validade do Consentimento:
 - ☑ Precisa ser concedido de forma livre – Ao titular deve ser conferido o poder de escolher se quer ou não informar seus dados;
 - ☑ Precisa ser informado – O titular deve ser munido de todas as informações sobre como seus dados serão tratados antes de concordar com o tratamento; e
 - ☑ Precisa ser inequívoco – O titular deverá consentir a partir de uma ação, seja por um clique na caixinha de “Li e concordo”, seja com a assinatura de um documento. A inércia do titular não será considerada como a concessão de um consentimento válido.

Mas nem sempre o consentimento é necessário, existem outras razões que abordaremos a seguir que autorizam o tratamento de dados, independentemente deste. Exemplos: na hipótese em que o titular fornece seus dados para passar por uma análise de crédito como medida preparatória para um contrato de locação, para receber uma proposta de prestação de serviços de administração imobiliária, ou, ainda, quando o fornecimento dos mesmos dados ocorre para que o contrato consiga ser cumprido.

- **Obrigação legal ou regulatória.** Nem sempre o tratamento depende exclusivamente do consentimento do titular de dados. Há leis e regulamentos que estabelecem o tratamento de dados pessoais como uma obrigação a ser cumprida pelo controlador, como, por exemplo, na hipótese em que um determinado condomínio precisa guardar os dados de seus colaboradores por um tempo pré-estabelecido em lei.
- **Execução de Contrato.** Esta base legal legitima o controlador a tratar os dados pessoais de um titular nos procedimentos que antecedem ou que ocorrem em decorrência da celebração de um contrato entre eles. Exemplo: na hipótese em que o titular fornece seus dados para receber uma proposta do controlador ou, ainda, quando o fornecimento dos mesmos dados ocorre para que o contrato consiga ser cumprido.
- **Processo judicial, administrativo ou arbitral.** Esta é a base legal mais indicada para legitimar um tratamento dos dados quando o objetivo do controlador é utilizar os dados pessoais do titular para exercer os seus direitos dentro de processos judiciais, administrativos ou arbitrais.
- **Proteção da vida e integridade física.** Esta base legitima o tratamento de dados pessoais em hipótese em que o titular ou um terceiro está em uma situação de risco à sua vida ou à sua segurança, como, por exemplo, quando o controlador utiliza tais dados para localizar o celular do titular e, com isso, viabilizar o seu resgate em uma situação de risco à sua vida ou integridade física.
- **Legítimo interesse do controlador ou de terceiros.** É certamente a mais flexível das bases legais. É por isso que deve ser adotada com especial cautela.

Esta base legitima o tratamento dos dados pessoais pelo controlador, quando, dentre outras hipóteses, a intenção é utilizar tais dados para apoiar e promover as suas atividades e de terceiros; ou realizar iniciativas que beneficiem o titular de dados. Ao contrário do consentimento, o controlador não precisa pedir a permissão do titular para tratar seus dados pessoais, o que não afasta a obrigação do controlador de deixar claras e transparentes as informações sobre esse tratamento. Isso porque, o titular não pode ser surpreendido pelas atividades de tratamento, devendo ter uma mínima expectativa de que ele ocorrerá. Um exemplo de utilização desta base legal é o que ocorre quando o titular fornece os seus dados pessoais de contato para que o corretor lhe apresente um determinado imóvel e, mais tarde, o corretor utiliza novamente os dados para apresentar ao titular uma oportunidade de negócio semelhante àquela apresentada anteriormente.

- **Proteção ao crédito.** Esta permite que instituições financeiras possam tratar os dados pessoais do titular, quando este está em busca de crédito. É uma das bases mais específicas previstas na LGPD, que não tem uma aplicação tão abrangente como as demais.

Quando o tratamento implicar a utilização de **dados pessoais sensíveis** – aqueles cujo tratamento sem o maior rigor poderia implicar riscos mais elevados ao titular, inclusive de discriminação –, as regras são um pouco mais restritivas e devem ser observadas com ainda maior atenção. Nessa hipótese, a LGPD dispõe que:

- O **legítimo interesse** e a **proteção ao crédito** não são bases aptas a permitir o tratamento de dados pessoais sensíveis.
- A base legal **execução de contrato** não está prevista entre as bases legais que autorizam o tratamento de dados pessoais sensíveis. Por outro lado, dentre tais bases há a previsão do **exercício regular de direito, inclusive em contrato**, o que de certo modo pode trazer efeitos práticos bem semelhantes, permitindo o tratamento dos dados pessoais sensíveis, quando imprescindíveis, no âmbito dos contratos.

- Há permissão para o tratamento de dados pessoais sensíveis para a garantia de **prevenção à fraude e segurança do titular**, hipótese em que o tratamento de dados pessoais sensíveis se mostra necessário nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Ela é adequada, por exemplo, para a utilização de dados biométricos como elemento de identificação, quando proporcionais às finalidades que motivam o tratamento.

Princípios do tratamento de dados

Os princípios do tratamento de dados são **valores que devem ser observados** sempre que se realizar uma atividade de tratamento. Esse é um requisito essencial que deve estar presente em todas as atividades que envolvam dados pessoais, e independentemente da base legal aplicada. São eles:

- **Finalidade** – o tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular de dados antes mesmo do seu início. Não é possível, por exemplo, alterar a finalidade no curso do tratamento dos dados, sem que tenha sido informado ao titular do dado tratado.
- **Adequação** – deve haver compatibilidade entre o tratamento e os propósitos legítimos e específicos informados ao titular.
- **Necessidade** – o tratamento deve ser restrito ao menor número de dados possíveis para atingir os propósitos informados ao titular. Não há espaço para a coleta de dados em excesso, menos ainda para o compartilhamento de dados excessivos. Esse raciocínio deve acompanhar a coleta de dados para acesso nos condomínios, a elaboração de atas, os registros em livros próprios, a concessão de acesso a terceiros sobre imagens e registros que não lhes digam respeito, devendo-se limitar o tratamento, que inclui, mas não se limita à coleta, ao compartilhamento e ao acesso ao mínimo possível de dados.
- **Livre acesso** – o titular deve ter garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento e, também, acesso à integralidade de seus dados pessoais.

- **Qualidade dos dados** – o titular deve ter a garantia de que seus dados pessoais tratados estão exatos, claros, atualizados de acordo com os propósitos que motivaram o seu tratamento.
- **Transparência** – ao titular devem ser garantidas as informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. O acesso a tais informações, em que pese seja uma garantia dos titulares, não é ilimitado, devendo preservar os segredos comerciais e industriais dos agentes de tratamento.
- **Segurança** – todos aqueles que tratam dados pessoais devem fazer uso de medidas técnicas e administrativas aptas a proteger os referidos dados de acessos indevidos, perdas e de situações acidentais ou ilícitas de destruição, alteração, comunicação ou difusão.
- **Prevenção** – quem trata dados pessoais deve adotar medidas para evitar danos aos titulares. Essas medidas não se restringem às medidas técnicas, sendo exigíveis também as medidas administrativas, como, por exemplo, o treinamento das pessoas que de qualquer modo tratarão dados pessoais. Eles devem saber sobre os limites impostos pela LGPD e sobre a sua obrigação legal de proteger os dados pessoais tratados.
- **Não discriminação** – os dados pessoais não podem ser tratados para fins discriminatórios ilegais ou abusivos.
- **Responsabilização e prestação de contas** – quem trata dados pessoais deve demonstrar a adoção de medidas de proteção de dados eficazes e que estejam de acordo com a LGPD.

Quais são as penalidades previstas na LGPD?

Desde **1º de agosto de 2021**, constatado o descumprimento da LGPD, a ANPD pode aplicar as penalidades administrativas descritas na própria lei. São elas:

- advertência;
- multa simples (de até 2% do faturamento do infrator, limitada a 50 milhões de reais);
- multa diária;
- possibilidade de tornar a infração pública;
- bloqueio dos dados pessoais envolvidos;
- eliminação dos dados pessoais envolvidos;
- suspensão parcial do banco de dados envolvido na infração, por um prazo de até 6 meses; e
- proibição parcial ou total de realizar atividades relacionadas ao tratamento de dados.

Para a imposição das penalidades administrativas acima, a ANPD relevará a gravidade e a natureza das infrações e dos direitos pessoais afetados, bem como algumas características e comportamentos do infrator.

As sanções administrativas, no entanto, são apenas parte das penalidades que podem ser aplicadas no caso de descumprimento da LGPD. Lembrando que, além de outras penalidades, o infrator poderá ainda ser obrigado a reparar eventuais danos materiais ou morais que vier a causar a partir do tratamento inadequado de dados pessoais.



CAPÍTULO II

ATIVIDADES MAIS COMUNS DE TRATAMENTO DE DADOS NO MERCADO IMOBILIÁRIO



O mercado imobiliário envolve uma ampla variedade de atividades de tratamento de dados. Embora muitas delas sejam específicas de determinado setor, por exemplo, de incorporação, de corretagem de imóveis ou de administração de condomínio, parte dessas atividades é comum a todos os envolvidos como, por exemplo, o gerenciamento dos dados de funcionários, contratação de fornecedores ou terceirizados, entre outras. Por isso, o objetivo deste capítulo é explorar os principais aspectos destas atividades e como elas se relacionam com a LGPD.

A. Tratamento de dados de colaboradores

Agora que a LGPD está em vigor, o que muda no tratamento dos dados dos colaboradores pela empresa?

Como em muitos pontos abordados neste e-book, a principal mudança no tratamento dos dados dos colaboradores pela empresa é a maior necessidade de **transparência** com os titulares de dados, já que a empresa é a **controladora** dos dados de seus funcionários. Uma série de atividades que já vinham sendo executadas anteriormente — como a supervisão de determinadas áreas utilizando câmeras de vigilância e o controle de presença por ponto (digital ou não) — continuam permitidas pela LGPD. Agora, porém, os colaboradores terão maior ciência de como estes tratamentos ocorrem e, a depender do caso, poderão exercer seus direitos enquanto titulares de dados. Nesse sentido, algumas medidas recomendadas são:

- Disponibilizar um **aviso interno de privacidade** — exclusivo para os colaboradores — que conceda informações sobre como seus dados pessoais são tratados;
- Realizar a **gestão adequada dos documentos dos colaboradores**, guardando-os em locais seguros e eliminando periodicamente os dados desnecessários e excessivos (o que pode ser feito conforme uma política de retenção de documentos); e
- Verificar e atualizar as **medidas de segurança técnicas e administrativas** utilizadas para proteger os dados pessoais dos colaboradores.

Qual a importância de um termo de confidencialidade?

O termo de confidencialidade deve **andar lado a lado com a proteção de dados** e tem como objetivo garantir que o colaborador respeitará o sigilo dos dados pessoais com que entrar em contato.

A obrigação de confidencialidade deve se **estender a todos os colaboradores (diretos e indiretos) e terceiros**, especialmente os que lidam com dados pessoais no dia a dia. A seguir, listamos alguns exemplos de funções que têm mais contato com os dados pessoais:

- consultores que lidam com clientes;
- profissionais do TI que cuidam da infraestrutura da empresa;
- corretores de imóveis que lidam diariamente com clientes;
- prestadores de serviço ou funções terceirizadas que lidam com dados pessoais.

Para novas contratações, recomenda-se incluir uma cláusula com previsões de confidencialidade e proteção de dados no contrato a ser celebrado.

Para contratos já existentes, essa obrigação pode ser incluída ou atualizada, geralmente por meio de um aditivo ao contrato ou pela celebração de um termo específico. O importante é que o colaborador assuma esta responsabilidade com a empresa.

Caso especial: corretores de imóveis

- Por terem uma atividade que lida com alto volume de dados pessoais, os corretores de imóveis precisam de cuidado especial com os dados pessoais de seus contatos (clientes, prospects, entre outros). Não raro, os corretores trabalham com sua própria base de clientes, formada ao longo dos anos, independentemente do relacionamento com alguma empresa imobiliária.
- Apesar de este relacionamento com clientes ser uma prerrogativa de sua profissão, os corretores devem tratar os dados pessoais com responsabilidade.
- É altamente recomendado incluir cláusulas de confidencialidade e proteção de dados nos contratos celebrados com os corretores, evitando que os dados pessoais sejam desviados de suas finalidades originais ou que configurem tratamento abusivo (e.g. envio de spam ou contatos não solicitados com o titular de dados).

Para maiores informações, consulte o Capítulo IV deste ebook.

O que são políticas de segurança da informação e qual a sua importância?

Além das políticas de proteção de dados e do acordo de confidencialidade, as políticas de segurança da informação são um **conjunto essencial de documentos** que contêm as diretrizes a serem seguidas para garantir que todas as informações — tanto dados pessoais quanto outras informações confidenciais — sejam devidamente protegidas, fomentando uma cultura de boas práticas de segurança da informação entre os colaboradores. Essas políticas regulam aspectos como:

- mesa e tela limpas (não manter documentos sigilosos na mesa de trabalho, nem abertos no computador; bloquear o computador ao sair da mesa);
- limitação de dispositivos autorizados a acessar os arquivos da empresa (por exemplo, não utilizar dispositivos particulares);
- meios adequados de compartilhar informações;
- limitações ao acesso de determinados sites e conteúdos no ambiente da empresa;
- política de retenção e descarte de documentos e mídias (*pendrives*, discos rígidos de computadores antigos, cópias de segurança etc.).

A Autoridade Nacional de Proteção de Dados lançou guia de segurança da informação para agentes de de pequeno porte que pode ser considerado o padrão mínimo de conduta e cuidados e pode ser acessado em <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf> Inclusive há um check list para auxiliar no mapeamento <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf>

B. Tratamento de dados de clientes

Como a empresa deve se preparar para lidar com dados de clientes?

Além de se adequar para com os colaboradores, a empresa também deve estar adequada para tratar dos dados de seus clientes. Para isso, alguns pontos importantes são:

- **Disponibilizar aviso de privacidade.** Também conhecido como “política de privacidade”, o aviso de privacidade é o documento que contém os principais pontos sobre como os dados pessoais do cliente serão tratados, incluindo seus direitos e como exercê-los.
- **Treinar sua equipe.** A equipe que lidará diretamente com os clientes (sejam os corretores parceiros, os colaboradores da própria empresa, entre outros) deve estar capacitada para realizar o atendimento em conformidade com a LGPD — o que inclui atualizações sobre:
 - como solicitar os dados pessoais dos clientes conforme a real necessidade para o objetivo do tratamento (por exemplo, não obrigar o cliente a fornecer seus dados para itens opcionais da contratação, como recebimento de *newsletters*); e
 - medidas de segurança utilizadas no cadastro dos dados dos clientes.
- **Gerenciar os dados dos clientes de maneira responsável.** Quando falamos em dados pessoais, menos é mais. É altamente recomendado que a empresa revise os dados que armazena e que solicita de seus clientes, para que mantenha somente as informações minimamente necessárias. Quantidades grandes de dados desnecessários e/ou desatualizados podem expor a empresa a maiores riscos de segurança da informação, principalmente no caso de vazamento de dados.

A LGPD autoriza o compartilhamento de dados dos clientes de uma empresa com parceiros comerciais?

Sim. O compartilhamento de dados pessoais é permitido pela LGPD. Ele, porém, precisa observar dois importantes requisitos:

1. ser justificado em uma **base legal adequada** (como o consentimento, o legítimo interesse, execução de contrato etc.); e
2. sempre **respeitar os princípios de tratamento** de dados, inclusive no que se refere à transparência e à segurança dos dados.

Uma empresa imobiliária, dependendo do seu ramo de atuação, pode compartilhar dados pessoais com as mais diversas finalidades, como, por exemplo:

- serviços de infraestrutura tecnológica – como servidores, armazenamento em nuvem, programas de CRM (*customer relation management*);
- serviços ligados a marketing, como agências de publicidade e de gerenciamento de mídia digital;
- serviços ligados a telemarketing ou central de contato da empresa (“Fale Conosco” ou “SAC”);
- iniciativas ligadas a parceiros comerciais, que incluam benefícios ou novidades aos clientes.

Independentemente do objetivo do compartilhamento, é **altamente recomendado formalizar as obrigações em um contrato** que inclua cláusula de privacidade e proteção de dados.

Se a empresa é a controladora dos dados dos clientes, isso significa que os colaboradores são operadores?

Não necessariamente. É comum haver confusão entre a relação de trabalho e as

funções dos agentes de tratamento. Mas não se engane. Ao tratar dados pessoais no exercício regular de suas funções dentro da empresa, os colaboradores estão agindo como agentes de seu próprio empregador — ou seja, eles são parte do próprio controlador, e não um terceiro contratado especificamente para tratar dados seguindo instruções do controlador. O operador seria, por exemplo, uma empresa contratada especificamente para tratar dados, como serviços de armazenamento em nuvem.

De qualquer modo, é importante lembrar que **nem todos os colaboradores têm o mesmo nível de acesso aos dados pessoais tratados**. É recomendado que esse acesso seja restrito aos colaboradores realmente necessários para o desempenho de função específica e que esses critérios sejam formalizados pela empresa, por meio de políticas e diretrizes internas, criadas por um comitê de privacidade ou órgão semelhante. Se você tem dúvidas sobre o seu papel ou o papel de seus funcionários em relação às atividades da empresa, não deixe de consultar um especialista em proteção de dados sobre o seu caso específico.

C. Relação com titulares de dados e com a ANPD

A contratação de um Encarregado (DPO) é obrigatória? Como proceder?

O Encarregado (ou DPO) é o responsável, dentro da empresa, por fazer a intermediação com a ANPD e os titulares de dados. A ANPD regulará, até o primeiro semestre de 2022, os detalhes sobre a obrigatoriedade de nomeação ou contratação de um DPO para empresas e pessoas jurídicas em categorias específicas.

A aplicação da LGPD para startups, empresas de pequeno porte e entes despersonalizados, nos quais se enquadram os condomínios, foi regulamentada pela ANPD recentemente (regulamentação cd/ANPD n. 2 de 27 de Janeiro de 2022) que dispensou a nomeação de DPO quando não se realiza tratamento de alto risco, mas obriga a existência de um canal para o exercício de direitos pelo titular. <https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>

Porém, a contratação ou a nomeação de um Encarregado para empresas que não se enquadrem nessa regulamentação ou não tenham certeza de realizar tratamento

de alto risco é medida recomendada, até para demonstrar o comprometimento de adequação à LGPD e de facilitar a comunicação com os titulares de dados.

Como agir diante de requisições de titulares de dados? É necessário ter um canal específico para esta finalidade?

O agente de tratamento deve estar preparado para receber e lidar com requisições de titulares de dados no decorrer de suas atividades. É indicado estabelecer um canal de contato específico para isso e treinar a equipe responsável sobre como lidar com tais requisições. Apesar de a lei prever o direito de o titular de dados obter certas informações imediatamente, isso não significa que toda e qualquer solicitação do titular de dados possa ser atendida — algumas vezes, será tecnicamente ou legalmente inviável atender ao titular. Independentemente do caso, o agente de tratamento deve sempre retornar ao titular, mesmo que seja para informá-lo da inviabilidade de atendê-lo.

D. Contratação de fornecedores e prestadores de serviço

Os fornecedores e prestadores de serviço precisam estar adequados à LGPD?

Sim. Isso é fundamental, principalmente se o fornecedor realiza atividades de algum modo ligadas ao tratamento de dados pessoais em nome da empresa.

- **Para contrato com um novo fornecedor,** leia o contrato cuidadosamente e verifique se possui uma cláusula sobre tratamento de dados e adequação à LGPD. Caso o contrato não tenha essa cláusula, sugira que seja incluída. Se for um serviço que lida principalmente com dados pessoais (por exemplo, prestação de serviço de segurança patrimonial e vigilância), é aconselhável, inclusive, consultar um especialista no assunto, para sugerir os aspectos mais importantes.
- **Para contratos já existentes,** é necessário atualizá-los, o que pode ser feito por meio de um aditivo ao contrato, que inclua cláusulas de proteção de dados e de adequação à LGPD. Em caso de dúvidas, não deixe de buscar o conselho de um especialista.

Que cuidados são necessários ao contratar produtos como *softwares* e sistemas?

As contratações que envolvem o tratamento direto de dados pessoais, como *softwares*, serviços de armazenamento e sistemas, necessitam de cuidados especiais. **Antes da contratação** é fundamental realizar uma análise profunda dos fornecedores disponíveis no mercado e do seu **nível de adequação à LGPD**, inclusive com as **medidas de segurança que oferecem** (por exemplo, se os dados são criptografados, se há transferência internacional de dados e para quais países). Como regra geral, é recomendado dar preferência para soluções **já estabelecidas no mercado** e que também operem em mercados com um alto padrão de proteção de dados, como ocorre na Europa com o *General Data Protection Regulation* (GDPR).

E. Segurança: controle de acesso

Quais cuidados devem ser tomados com o controle de acesso ao edifício via cartão ou crachá?

As empresas possuem um interesse legítimo em proteger sua segurança e limitar o acesso às áreas internas para pessoas autorizadas. Um cartão de acesso é uma medida eficiente de autenticar a identidade do titular, mas é necessário tomar uma série de cuidados para evitar que o cartão se torne um ponto fraco na segurança. A exemplo de outras medidas restritivas de acesso, deve-se verificar até que ponto a interferência nos direitos do titular é justificável.

Para isso, é interessante realizar uma **Análise de Legítimo Interesse**, uma boa prática de proteção de dados recomendada no âmbito do Regulamento Geral de Proteção de Dados europeu e por diversas autoridades de proteção de dados europeias. Embora não esteja prevista expressamente na LGPD, a Análise de Legítimo Interesse é um estudo composto por três avaliações: **(i)** se há de fato um interesse legítimo, **(ii)** se o tratamento pretendido é necessário e **(iii)** se a interferência nos interesses e direitos do titular de dados é proporcional ao fim que se pretende atingir. A Análise de Legítimo Interesse pode ser usada para fins de auditoria, a fim de justificar a adoção de cartões de acesso.

Como qualquer medida de segurança envolvendo dados pessoais, o registro do cartão deve estar associado a **protocolos de segurança** que permitam que o cartão seja desativado tão logo a equipe de segurança seja alertada de algum problema pelo titular (perda, roubo ou extravio). O cartão também deve estar ligado aos dados pessoais minimamente necessários para identificar o portador, de modo a prevenir riscos de segurança.

O que é importante saber sobre monitoramento por câmeras?

O monitoramento por câmeras é muito importante para a segurança da empresa e de condomínios em geral, mas precisa ser feito com cuidado para não invadir injustamente a privacidade das pessoas que circulam por aquele espaço.

A **posição adequada das câmeras** deve considerar tanto os ambientes internos do edifício quanto a área externa. No caso de condomínios, elas não devem captar imagens de áreas privadas como dentro das unidades ou de banheiros disponíveis nas áreas comuns, e não podem cobrir uma área externa além das redondezas necessárias para garantir a segurança do edifício. O mesmo vale para os edifícios comerciais e até mesmo para a própria sede da empresa.

As imagens (e eventuais áudios) devem ser guardadas seguindo **protocolos de segurança** e **não podem ser retidas por um tempo longo demais**. Caso as câmeras usem redes sem fio ou internet, é importante que elas contem com medidas técnicas de segurança, como a criptografia, para evitar que seu conteúdo seja interceptado. Além disso, o **acesso às imagens deve ser limitado às pessoas autorizadas** (síndico, encarregado da segurança, porteiro/vigia, entre outros). A **definição de quem serão essas pessoas** autorizadas pode variar conforme a natureza do condomínio ou edifício, o fluxo de pessoas e os responsáveis pela gestão e segurança do local. De qualquer modo, recomenda-se que este ponto seja formalizado em documento específico, como política interna, diretriz, convenção condominial ou instrumento semelhante.

Por fim, **não esqueça de sinalizar os lugares que são gravados por câmeras!**



CAPÍTULO III

A ATIVIDADE DE INCORPORAÇÃO



A atividade de incorporação tem algumas peculiaridades, principalmente porque lida com os interesses de diversos agentes e exige um grande número de documentos para a sua regularização. Por isso, muitos tratamentos de dados que realiza são justificados pela base legal do cumprimento de obrigação legal ou regulatória.

A. Regularização da incorporação

Que cuidados a incorporadora deve ter ao lidar com os documentos necessários para regularizar a incorporação?

Os documentos utilizados na regularização da incorporação também são fonte de muitos dados pessoais. Além disso, vale lembrar que a LGPD não se aplica somente para dados tratados no meio digital ou eletrônico — mas, também, nos meios físicos. Por isso, a incorporadora deve adotar medidas para garantir que estes documentos físicos estejam protegidos e bem acondicionados. Ainda, recomendamos que a incorporadora utilize uma **política de guarda e retenção de documentos**, para verificar quais documentos ainda precisam ser mantidos e quais podem ser eliminados.

Uma vez regularizada a incorporação e as vendas estejam prontas para iniciar, quais cuidados a incorporadora deve ter ao procurar potenciais compradores? Com quem os dados podem ser compartilhados?

No próximo capítulo, abordaremos bastante os cuidados para uma correta prospecção de clientes. De qualquer modo, já adiantamos que a **transparência com o cliente** é fundamental. Ele precisa ter uma expectativa mínima de que seus dados serão compartilhados com terceiros — geralmente parceiros comerciais — e que estes parceiros podem fazer ofertas que, potencialmente, sejam do seu interesse.

Que cuidados a incorporadora deve ter em se tratado da assembleia de instalação do condomínio que ocupará o empreendimento?

A assembleia de instalação do condomínio é uma oportunidade em que é tratado

um volume considerável de dados pessoais, a maioria deles com a finalidade de **cumprir obrigações legais ou regulatórias** associadas a um novo condomínio. Mesmo que o empreendimento esteja finalmente ganhando vida, é importante que a incorporadora ainda tome as devidas providências para que o tratamento dos dados pessoais dos envolvidos seja realizado de maneira segura e transparente.

Antes do início da assembleia, recomenda-se que os participantes sejam avisados da finalidade do tratamento dos dados (ou seja, viabilizar a própria assembleia). No mais, caso haja situações que envolvam a contratação de prestadores de serviço que lidem, de algum modo, com dados pessoais, é fundamental formalizar as obrigações e responsabilidades das partes, bem como dar ciência aos condôminos sobre esta contratação.

Uma vez que o condomínio esteja instalado e operando normalmente, a incorporadora ainda possui algum dever de compartilhar dados com o síndico ou outros envolvidos com o condomínio?

A resposta a esta pergunta depende muito do caso, mas **via de regra**, não. Uma vez instalado o condomínio, entende-se que ele já possui todos os subsídios para funcionar por conta própria. Por isso, pedidos de síndicos para compartilhamento de dados de proprietários das unidades, por exemplo, só devem ser atendidos se houver uma justificativa para tanto, acompanhada de uma base legal adequada. Esses dados podem ser obtidos de fontes mais apropriadas, seja por meio da própria administradora contratada ou a partir dos dados já compartilhados pela incorporadora no momento da instalação do condomínio.

B. Vendas e atuação de corretores associados

Quais cuidados devem ser adotados nos estandes de vendas de empreendimentos imobiliários?

Por serem a porta de entrada para muitos clientes, os estandes de venda também lidam com grandes volumes de dados pessoais de possíveis clientes e aqueles

que efetivamente fecharão um negócio. É uma etapa do negócio em que se deve ter especial cuidado e demonstrar evidências de que a empresa está adequada à LGPD. A seguir, elencamos algumas dicas para facilitar este trabalho, sem prejuízo da observação do disposto no Capítulo IV – A Atividade de Intermediação de Vendas e Locação.

- **Treine os colaboradores e demais responsáveis por lidar com os dados pessoais.** Elabore um treinamento prático com as informações e orientações necessárias para que o colaborador possa lidar com os dados pessoais dos possíveis clientes com responsabilidade e segurança. Em geral, este treinamento deve abordar pontos como: o modo de informar o titular de dados sobre o motivo pelo qual os seus dados devem ser coletados e como poderão ser utilizados; medidas de segurança no manuseio de fichas cadastrais, documentos e no acesso a sistemas; para quais finalidades e como os dados pessoais poderão ser compartilhados, entre outros.
- **Celebre um acordo de confidencialidade específico com os colaboradores alocados para trabalhar nos estandes,** de modo que eles se comprometam com a confidencialidade dos dados pessoais e de informações aos quais venham a ter acesso, não os compartilhando de maneira indevida.
- **Disponibilize um aviso (política) de privacidade facilmente acessível para os visitantes do estande.** É importante que se garanta a transparência aos titulares de dados quanto ao tratamento de dados pessoais que poderá ser realizado em virtude da sua visita ao estande, desde o momento da coleta destes dados na recepção do local. Uma boa maneira de fazer isso é disponibilizar um QR code em local de destaque, de modo que o visitante poderá escaneá-lo com seu próprio celular e acessar o aviso de privacidade. Também é interessante manter uma versão física resumida, que aborde os principais pontos (a finalidade do tratamento, quais dados serão utilizados, os direitos do titular e como entrar em contato com o DPO).
- Priorize estandes de autoatendimento e suporte digital (como tablets) para coleta dos dados. Com fichas em papel e atendimento humano, há maiores riscos de que os dados sejam perdidos ou acessados por pessoas indevidas.

Assim, a coleta e o armazenamento das informações por vias digitais permitem uma integração direta com os sistemas da empresa e uma maior segurança para os dados em geral.

Para a divulgação on-line de empreendimentos, quais os principais cuidados que devem ser tomados?

Os canais on-line podem ser grandes aliados na divulgação de novos empreendimentos. Em geral, os cuidados para esta divulgação são muito semelhantes com os que mencionamos em outros casos de tratamento de dados pessoais, mas não custa lembrar aqui os principais:

Priorize a transparência, disponibilizando um aviso (ou política) de privacidade.

Além das informações essenciais sobre o tratamento, é importante que este aviso seja escrito de maneira acessível para o titular de dados, que poderá consultá-lo a qualquer tempo, desde o primeiro momento de acesso ao canal. O melhor modo de elaborá-lo depende da estratégia adotada pela incorporadora: pode ser o aviso já utilizado pela incorporadora a nível institucional, um documento específico para aquele empreendimento, entre outras possibilidades, considerando as particularidades dos dados que serão coletados e as finalidades de sua utilização dentro do contexto do canal.

Se a divulgação for realizada também por parceiros comerciais, estabeleça diretrizes de uso de dados pessoais e de uso de marca, a fim de que o titular de dados saiba quem são os envolvidos no tratamento. Estas diretrizes podem ser estabelecidas diretamente no contrato com o parceiro, incluindo cláusulas de propriedade intelectual e de proteção de dados. Isso é importante para evitar os casos em que empresas de menor porte se utilizam de marcas alheias para atrair mais clientes — o que tem grandes chances de causar confusão no titular de dados e ele responsabilizar o agente errado por eventuais danos que possa sofrer em virtude de eventual tratamento de dados indevido.

No caso de corretores associados que trabalham com bases de dados próprias, que cuidados tomar para garantir que o tratamento de dados está em conformidade com a LGPD?

É comum que corretores associados a incorporadoras tenham também a sua própria base de clientes, conquistada no decorrer do tempo de sua atuação — e, muitas vezes, não relacionada ao seu vínculo atual com uma incorporadora. A relação neste caso é um tanto delicada, pois os corretores possuem autonomia sobre a sua própria base de clientes. Mas existem alguns cuidados que a incorporadora pode adotar para tornar essa relação mais segura e proveitosa:

- **Celebrar termo de responsabilidade com o corretor associado**, por meio do qual ele se compromete a somente compartilhar dados que foram obtidos em conformidade com a LGPD. Neste termo, o corretor também pode se responsabilizar pela origem lícita dos dados.
- **Registrar a origem de todos dos dados inseridos e extraídos de sistemas de gerenciamento de clientes** utilizados pela incorporadora, a fim de facilitar a identificação da origem/fonte daqueles dados, bem como verificar quais corretores puderam acessá-los.
- **Criar políticas internas de restrição de acesso e gerenciamento dos dados pessoais**, a fim de evitar que os dados de clientes registrados em sistemas de gerenciamento sejam extraídos ou alterados sem controle e evidências. Esta medida também é interessante para evitar que a base de dados existente seja extraída de maneira indevida e compartilhada com terceiros e/ou concorrentes.
- **Realizar treinamentos e capacitações em proteção de dados** com estes corretores, para informá-los sobre as normas da companhia e fortalecer a cultura de proteção de dados envolvendo também este aspecto na atuação do corretor.
- **Informar aos titulares de dados sobre a participação e responsabilidade do corretor no tratamento de suas informações**, o que poderá estar disposto no Aviso de Privacidade, deixando claro o envolvimento dos corretores associados

no tratamento de dados, especialmente na coleta e no compartilhamento de informações, bem como a ligação destes corretores com a incorporadora.

Com esta é uma atividade recorrente em outros ramos da indústria imobiliária, veja nossas recomendações também no Capítulo IV – A Atividade de Intermediação de Vendas e Locação, em que trazemos outras dicas importantes que também se aplicam para o ramo da incorporação.

C. Outros casos de compartilhamento de dados

Até que ponto os dados de clientes podem ser compartilhados com parceiros comerciais da incorporadora?

Enquanto **controladora dos dados pessoais de seus clientes**, a incorporadora tem o poder de decisão sobre como estes dados serão tratados. Mas esse tratamento deve seguir o disposto na LGPD, com especial atenção para a **transparência com o titular de dados**. Por isso, a incorporadora pode compartilhar os dados de seus clientes nas situações em que entender que isto é relevante para seu negócio, mas que não representa uma interferência indevida nos direitos deles enquanto titulares de dados.

O compartilhamento de dados de maneira responsável geralmente envolve um ou mais pontos dentre os listados a seguir:

- o titular de dados tem fácil acesso a informações importantes sobre esse compartilhamento (por exemplo, estão no aviso de privacidade da incorporadora), permitindo que ele esteja ciente ou ao menos tenha a expectativa de que esse compartilhamento de seus dados será realizado;
- a atividade possui uma base legal adequada ao caso específico;
- o titular tem alguma possibilidade de comunicar caso não queira mais que seus dados sejam tratados daquela maneira — seja por meio da revogação do seu consentimento (caso tenha sido coletado) ou da possibilidade de oposição ao tratamento.

Em casos de fiscalização da execução das obras, é permitido compartilhar os dados dos colaboradores e prestadores de serviço envolvidos quando solicitado?

Esse compartilhamento **dependerá muito do contexto**. Existem casos em que a incorporadora de fato necessita compartilhar tais dados para **cumprir obrigações legais ou regulatórias** — por exemplo, um pedido de uma autoridade fiscalizadora. Porém, nos casos em que esse compartilhamento não decorre de uma obrigação legal, é importante obter do solicitante informações sobre o motivo para o compartilhamento e que uso ele dará aos dados. Caso o solicitante não seja capaz de dar informações satisfatórias, recomenda-se não compartilhar os dados dos colaboradores, a fim de resguardar sua privacidade e garantir que as obrigações da legislação de proteção de dados não sejam violadas. Não deixe de consultar um especialista em proteção de dados quando tiver dúvidas sobre essas solicitações.

Se um cliente adquiriu um produto imobiliário diretamente com outra empresa, mas a incorporadora está envolvida na execução do projeto, é possível compartilhar os dados desse cliente?

Na maioria das vezes, sim. Mesmo que o cliente tenha adquirido o produto imobiliário por outros meios, frequentemente a incorporadora necessita dos dados dele para viabilizar a construção e entrega do imóvel — ou seja, para **executar o contrato celebrado com este cliente adquirente**. Nestes casos, é importante que o cliente esteja ciente deste compartilhamento de dados e de que ele só ocorre para viabilizar um contrato a pedido dele mesmo.



CAPÍTULO IV

A ATIVIDADE DE INTERMEDIACÃO DE VENDAS E LOCAÇÃO



A. Prospecção de clientes e bases de dados

A LGPD autoriza a prospecção de clientes? Quais são as limitações?

A LGPD não impede que uma empresa realize prospecção de clientes ou utilize outros mecanismos de *marketing* para fomentar seu negócio. Além disso, faz parte das atribuições do corretor de imóveis a prospecção de possíveis interessados. Porém, esse uso dos dados de potenciais clientes exige um grande **respeito aos direitos do titular**. A seguir, listamos alguns cuidados fundamentais para na primeira abordagem com os potenciais clientes:

- **Verificar a fonte da base de contatos.** Ao adquirir bases de dados de terceiros para fins de segmentação, é necessário verificar se estes dados **foram obtidos de maneira lícita** pelo fornecedor. Informe-se junto ao fornecedor qual a base legal utilizada para construir aquele banco de dados: **(i)** Se foi o consentimento, ele foi obtido de maneira válida, livre e informada? **(ii)** Se foi o legítimo interesse, o titular foi informado dessa finalidade? Como medida de precaução, é altamente recomendado formalizar no contrato com o fornecedor que ele garante e responde pela licitude dos dados pessoais, inclusive pela coleta adequada e pela disponibilização de informações claras aos titulares de dados sobre seus direitos.
- **Prospecção consciente.** Quando o objetivo da campanha é atingir novos potenciais clientes, é bem possível que o destinatário fique surpreso com um e-mail sobre um novo empreendimento imobiliário. Para evitar situações como esta e respeitar a privacidade do titular, é recomendado que mensagens de contato inicial não contenham, desde o seu primeiro momento, promoções ou condições especiais, mas, sim, que perguntem ao titular se tem interesse em receber comunicações do tipo. Caso o destinatário não responda ou não abra o e-mail, é melhor não insistir no envio de novas mensagens.
- **Ser transparente.** Toda mensagem enviada ao titular de dados deve conter uma breve explicação de porque ele a recebeu e como pode fazer para se descadastrar (por exemplo, "Você recebeu este e-mail porque faz parte de nossa lista de contatos"). Também é recomendado haver um link com o aviso (ou

política) de privacidade, para que o titular tenha acesso a mais informações sobre como seus dados são tratados.

- **Mecanismo de *opt-out* eficiente.** O *opt-out* é um mecanismo que permite ao destinatário da mensagem sinalizar que não deseja receber mais e-mails daquele tipo (geralmente localizado ao final da mensagem). Independentemente da base legal utilizada para justificar o envio das mensagens, é recomendável que elas contenham um *opt-out* eficiente, que de fato descadastre o destinatário daquela *mailing list*.
- **Reciclagem e respeito à finalidade de tratamento.** Uma *mailing list* desatualizada, repleta de contatos que não retornam, pode representar um risco maior à segurança em caso de vazamentos ou incidentes do tipo. Por isso, recomenda-se que a *mailing list* seja revista periodicamente e atualizada para manter os dados de titulares que de fato tenham demonstrado interesse em receber as comunicações, ou que demonstrem potencial para isso. No mais, dados desnecessários e desatualizados devem ser eliminados permanentemente.

É possível utilizar os dados de um cliente para informá-lo de outros empreendimentos futuros?

Sim, é possível, desde que esse cliente tenha o mínimo de expectativa de que estes contatos posteriores poderão ocorrer. É neste caso que as *mailing lists* e *newsletters* são úteis e perfeitamente justificadas pela base legal do legítimo interesse. Porém, como apontado na questão acima, caso o cliente/titular de dados tenha manifestado de alguma forma que não deseja receber este tipo de contato (por meio do *opt-out*, por exemplo), então ele não deve ser contatado.

É possível filtrar os titulares por determinados atributos (como renda) sem que isso configure como discriminação?

Sim, é possível. Essa segmentação da base de titulares é considerada uma formação de perfil. Quando se utiliza um tratamento como esse, é fundamental respeitar o

princípio da não-discriminação: os dados pessoais não podem ser utilizados para fins ilícitos, abusivos ou injustos para o titular em relação aos demais. Por isso, para fins de auditoria, recomendamos delimitar de maneira clara estes critérios, caso essa segmentação seja questionada. Além disso, ela pode ser justificada por uma série de fatores, inclusive nas legítimas expectativas do titular (por exemplo, titulares com maior renda poderiam ter a expectativa de receber e-mails sobre empreendimentos de alto padrão em áreas mais valorizadas da cidade).

Há algum cuidado especial com dados disponíveis publicamente? Eles podem ser utilizados para fins de prospecção de clientes?

Os dados públicos, ou tornados públicos voluntariamente pelo titular, podem ser tratados para outras finalidades, como de marketing, por exemplo. Mas isso não significa que eles podem ser usados sem qualquer critério. Esse novo tratamento deve considerar as expectativas do titular e respeitar os princípios da LGPD, principalmente da transparência, da finalidade e da não-discriminação. Ou seja, aqui valem os mesmos cuidados indicados no uso de *mailing lists* e bases de terceiros. Além disso, é sempre importante avaliar se a finalidade que justificou a publicização do dado pessoal guarda relação com o novo tratamento.

Campanhas de Indicação: como organizá-las em conformidade com a LGPD?

As campanhas de indicação são excelentes oportunidades para corretores de imóveis e imobiliárias em geral. Com a LGPD em vigor, o regulamento dessas campanhas deve contemplar não apenas a dinâmica de eventuais premiações, mas, também, transparência nas questões relacionadas aos dados pessoais compartilhados. Dicas importantes são:

- **Minimização de dados.** Para que o participante possa indicar um imóvel para a campanha, recomenda-se que seja exigido o mínimo de dados possível — ou seja, somente o necessário para identificar o imóvel e seu proprietário.

- **Verificação do consentimento do proprietário do imóvel (ou profissional indicado).** Por se tratar de uma iniciativa de *indicação*, e não de ação do próprio titular, o consentimento do indicado é importante, a fim de respeitar as legítimas expectativas do indicado. O formulário de participação deve contemplar uma coleta de consentimento dele (seja por assinatura, pelo preenchimento de uma *checkbox* ou meio idôneo semelhante).
- **Respeito às finalidades de coleta dos dados.** Campanhas nesses moldes podem atrair diversos participantes, como corretores independentes. Caso a idealizadora da campanha pretenda criar uma oportunidade de relacionamento continuado com o participante, recomenda-se: **(a)** disponibilizar um *opt-in* para que o participante comunique se deseja ou não receber outros comunicados, ou **(b)** esclarecer que o participante poderá receber mensagens publicitárias, mas tem a opção de se descadastrar a qualquer tempo (*opt-out*).

B. Diligências do corretor

A LGPD permite a verificação de dados do comprador do imóvel? Como justificar o tratamento desses dados?

A LGPD **não impede a verificação de dados do potencial comprador de imóveis**. Como estamos falando de uma relação contratual, práticas como checagem de débito e solicitação de documentos do potencial comprador podem ser justificadas pela base legal da **execução de contrato**, já que é do interesse do comprador adquirir o imóvel. Porém, a verificação destes dados não pode ser excessiva; ou seja, o corretor só deve analisar **os dados estritamente necessários** para a celebração do contrato e, ainda, quando voltadas às providências preliminares ao contrato devem partir da solicitação do próprio titular.

O corretor pode receber os documentos necessários para fechar o negócio em seu número particular de WhatsApp (ou serviço de mensageria equivalente)?

Não é recomendável. Ao lidar com documentos e informações necessárias para a conclusão do negócio, todo o trânsito dessas informações deve ocorrer pelos meios oficiais disponibilizados pela corretora — como e-mail e número de WhatsApp profissional, por exemplo. Utilizar meios externos de comunicação pode expor a empresa a grandes riscos de segurança da informação, especialmente caso um colaborador que adote estas práticas seja desligado por algum motivo. Quem vai garantir que ele está mantendo as informações dos clientes protegidas, ou que não compartilhará com terceiros de forma a contrariar as normas de segurança da informação da empresa?



CAPÍTULO V

ADMINISTRAÇÃO DE LOCAÇÃO



A. Avaliação de risco do locatário

Quais cuidados são necessários com os documentos do candidato a locatário?

O processo de avaliação de crédito e verificação de riscos do locatário envolve uma série de documentos, contendo os dados financeiros do indivíduo e de terceiros que serão seus fiadores. Neste processo, é normal que o locador tenha acesso, em alguma medida, a essas informações. Entretanto, esse acesso não deve ser livre e irrestrito. Ao intermediar essa relação, é **papel da imobiliária filtrar essas informações** e compartilhá-las com o locador na medida do necessário, para que ele tenha os subsídios para a decisão de aceitar ou não o candidato a locatário, ao mesmo tempo que a privacidade deste e dos fiadores é respeitada.

Assim como em outros exemplos deste *e-book*, **os documentos devem ser armazenados de maneira segura**, seguindo os protocolos de segurança da imobiliária, e com **acesso restrito às pessoas autorizadas**. Além disso, os documentos não podem ser mantidos indefinidamente: uma vez atingida a finalidade do tratamento desses dados, tais documentos devem ser adequadamente descartados, para evitar o armazenamento de dados pessoais desnecessários.

Caso o perfil do candidato a locatário seja recusado, devo informar a ele os motivos da recusa?

Via de regra, sim. Como parte dos seus direitos como titular de dados, o candidato a locatário que teve seu perfil recusado tem o direito de obter o mínimo de informação sobre o motivo da recusa. **Isso, porém, não significa que a imobiliária precisa expor todo o seu processo de análise:** basta informar ao indivíduo, sucintamente, qual foi o motivo relevante da decisão.

B. No decorrer do contrato

Quais cuidados são necessários nos momentos de entrega das chaves? É permitido verificar a identidade de quem as está retirando?

O responsável por administrar o contrato de locação tem o direito e a responsabilidade de ser zeloso com o imóvel sob sua administração. **Não há qualquer impedimento à verificação da identidade da pessoa que retirará ou entregará as chaves**, por exemplo. Esse é um tratamento de dados pessoais necessário para viabilizar a **execução do contrato** celebrado com o locatário.

É correto utilizar redes sociais e/ou aplicativos de mensageria para realizar comunicados importantes sobre a administração da locação?

Com a variedade de aplicativos de mensageria e e-mail de hoje em dia, a transmissão de informações e documentos ficou mais rápida e conveniente. Porém, ainda se faz necessário um cuidado especial quando essas mensagens envolvem informações sobre locação e dados pessoais. Algumas medidas recomendadas:

- deixar as redes sociais somente para mensagens promocionais — qualquer outro comunicado importante deve ser feito por outro meio;
- **não utilizar contas pessoais ou particulares** de aplicativos para se comunicar com o locatário;
- priorizar um **canal oficial** (e.g. conta comercial ou profissional de aplicativos de mensageria) para comunicados importantes;
- priorizar o uso de e-mails corporativos da imobiliária para enviar e/ou receber documentos da parte do locatário.

Em caso de cobranças e ações judiciais, como lidar com os dados pessoais dos envolvidos?

As cobranças e ações judiciais geralmente são contextos em que o uso de dados pessoais é necessário para **viabilizar o exercício de um direito** — a saber, o do credor de obter o adimplemento da obrigação. Em geral, essas atividades envolvem o compartilhamento de dados pessoais por diversos meios e para diferentes destinatários e, por isso, exigem certos cuidados. A seguir, listamos os principais:

- **Utilizar somente os dados estritamente necessários.** Mesmo que seja um procedimento complicado para os envolvidos, as cobranças judiciais ou extrajudiciais devem envolver apenas os dados realmente necessários para viabilizar a finalidade pretendida. Qualquer dado pessoal que não seja realmente útil no atingimento deste resultado deve ser imediatamente excluído.
- **Compromisso de confidencialidade e cuidado com os dados pessoais.** Mesmo que a cobrança motive uma ação judicial, não há justificativa para expor os envolvidos ou utilizar seus dados pessoais de maneira indevida. Ao contratar escritórios de advocacia, agências de cobrança, entre outros, é fundamental que haja uma cláusula ou termo de proteção de dados, responsabilizando os agentes de tratamento envolvidos pelos seus atos, e incentivando-os a adotar medidas de segurança (tanto técnicas quanto gerenciais) apropriadas para manter os dados efetivamente protegidos.
- **Usar canais de comunicação seguros.** Conforme explicamos na questão sobre aplicativos de mensageria e redes sociais, quando estamos falando em procedimentos de cobrança ou ações judiciais, é preciso cautela ao escolher o meio de transmitir esses documentos e mensagens. Recomenda-se que a comunicação entre os envolvidos ocorra preferencialmente por meios de contato (e-mail, telefone, celular) profissionais, e não pessoais, bem como que sejam envolvidas somente as pessoas realmente necessárias neste contexto.

C. Contratação de terceiros

Que cuidados são necessários com a contratação de concessionárias e prestadores de serviços?

No que tange ao tratamento de dados pessoais, os cuidados necessários para este ponto não são diferentes das medidas recomendadas para outras relações contratuais envolvendo prestadores de serviço, fornecedores ou parceiros comerciais em geral. Relembrando:

- contrate prestadores de serviço que estejam em conformidade com a LGPD, ou seja, cujas operações estejam adequadas à lei;
- negocie sempre uma cláusula contratual ou termo de proteção de dados, por meio do qual a concessionária se responsabiliza pelo integral cumprimento das leis de proteção de dados aplicáveis, especialmente a LGPD, bem como pelas perdas e danos causados à administradora, ao locador ou a qualquer terceiro.

Quais cuidados devem ser tomados ao contratar terceiros para a execução de obras?

Em termos de proteção de dados, aplicam-se as mesmas recomendações feitas no Capítulo II. Para o contexto da atividade de administração, destaca-se a necessidade de conferir se o prestador de serviços está em conformidade com a LGPD, principalmente no que se refere à segurança da informação e ao dever de confidencialidade, a depender da natureza do serviço.



CAPÍTULO VI

ADMINISTRAÇÃO DE CONDOMÍNIOS



A. Gerenciamento de dados de condôminos

A LGPD permite compartilhar dados de condôminos?

Sim. Para a administração do condomínio, é normal que determinados dados dos condôminos ou residentes sejam compartilhados com prestadores de serviço ou fornecedores. Mas esse compartilhamento não deve ser indiscriminado: em todos os casos, é necessário **transparência com o titular** sobre com quem o dado é compartilhado, o porquê do compartilhamento e, ainda, a minimização dos dados pessoais objetos do compartilhamento. Além disso, é fundamental que ambas as partes (o remetente e o destinatário dos dados) estejam com suas obrigações em dia em relação à LGPD e aos direitos dos titulares.

Relembrando algumas dicas para casos de compartilhamento:

- verifique se o fornecedor ou prestador de serviço tem operações e serviços adequados à LGPD;
- negocie uma cláusula ou termo pelo qual o contratado se comprometa com as principais obrigações previstas na LGPD;
- informe aos titulares de dados sobre esse compartilhamento e disponibilize um canal de comunicação para que eles possam entrar em contato, tirando dúvidas sobre esse tratamento.

No portal eletrônico da administradora, quem deve ter acesso aos dados pessoais dos condôminos?

Idealmente, o acesso a ferramentas de gestão do condomínio, como o portal da administradora, deve ser **restrito às pessoas estritamente necessárias**, como seria o caso do síndico e os membros do corpo diretivo. Recomenda-se que esse assunto seja analisado pelo síndico e formalizado no instrumento apropriado do condomínio e do contrato com a administradora, priorizando que o acesso aos dados dos condôminos seja liberado ao próprio síndico e aos membros do corpo

diretivo. Demais solicitações devem ser analisadas caso a caso, para não comprometer a segurança destes dados.

Como lidar com as questões relacionadas à inadimplência de condôminos?

A LGPD não veio para interferir na relação entre o condômino e o condomínio, mas apenas para tornar algumas questões mais claras. Assim, recomendamos cuidado com a minimização dos dados na pasta de prestação de contas: que as informações sobre o assunto sejam registradas somente com o número da unidade.

Se o condomínio utiliza o formato digital para disponibilizar as pastas de prestação de contas, que dados podem ser exibidos e quais devem ser preservados?

A disponibilização dos resultados da prestação de contas deve traçar um equilíbrio entre a **transparência** e a **privacidade dos condôminos**. Ao divulgar esses resultados aos condôminos, considere fatores como a natureza do condomínio, seu tamanho, o número de condôminos, entre outros, e pergunte-se: **divulgar este dado pessoal é importante para a informação que quero disponibilizar a todos?** Isso é uma análise que deve ser feita caso a caso, mas, em geral, recomenda-se divulgar sempre o mínimo possível de dados pessoais, substituindo informações que identificariam a pessoa imediatamente por outras não tão diretas — por exemplo, fazer referência ao número da unidade e não ao seu morador (ou proprietário) em determinados casos.

Sobre os grupos de condôminos em aplicativos de mensageria (como WhatsApp): que informações podem ser compartilhadas? Qual a responsabilidade do síndico e/ou do administrador pelo que é falado ali?

Os grupos de condôminos em aplicativos de mensageria (WhatsApp, Telegram, Messenger, entre outros) servem como espaços muito úteis de comunicação entre os condôminos e moradores. Porém, não é raro vermos notícias de alguma questão séria que começou nesses grupos e tomou tais proporções a ponto de render ações

judiciais com os envolvidos. Nesses casos, o **administrador do grupo pode ser responsabilizado** se não intervir nos conflitos que venham a surgir. Assim, para garantir que o grupo de mensagens seja um espaço de diálogo e respeito entre todos, elencamos algumas sugestões a seguir:

- institua um grupo como o “oficial” do condomínio, voltado exclusivamente para este assunto;
- deixe as regras do grupo claras para todos os participantes (por exemplo, colocando na descrição do grupo ou enviando diretamente aos membros novos);
- limite o compartilhamento de dados e mídias dentro e fora do grupo, para evitar que os assuntos ali tratados sejam expostos de maneira indevida;
- limite o assunto do grupo — ou seja, se houver condôminos interessados em outros temas, encoraje-os a criar seu próprio grupo, independentemente do grupo oficial;
- a depender da natureza do condomínio, considere também utilizar o grupo oficial como uma lista de transmissão — ou seja, somente o administrador manda mensagens, os demais membros apenas as visualizam.

Por fim, mesmo que o grupo do condomínio contenha o síndico e os membros da administração, recomendamos que esse não seja o único canal institucional de comunicação com os condôminos. Considere também outros meios, como **e-mails institucionais**, que ainda são utilizados por muitos condomínios.

B. Assembleia de condôminos

Nas ocasiões em que a assembleia de condôminos é gravada, as imagens podem ser compartilhadas a pedido de um condômino?

Via de regra, não. A principal finalidade do registro eletrônico das assembleias de condôminos, principalmente as realizadas por meio da tecnologia (ou seja, não

presenciais), é servir como subsídio para a redação da ata da reunião. Recomenda-se que esta finalidade seja comunicada aos condôminos **antes do início de cada assembleia**, para que todos tenham ciência do motivo do registro.

Para a correta condução dos trabalhos, o **presidente e o secretário podem solicitar as imagens**, desde que assumam o compromisso — por meio de termo de responsabilidade ou instrumento semelhante — de utilizar estes registros somente para a elaboração da ata, e nenhuma outra finalidade estranha a este escopo. Após, estas imagens devem ser descartadas da maneira adequada, de modo que não sejam utilizadas para finalidades posteriores. Portanto, essas imagens não devem ser compartilhadas a pedido de um condômino, pois contém dados de terceiros considerados sensíveis e não condiz com a finalidade da gravação.

A lista de presença da assembleia necessita ser registrada juntamente com a ata?

Sim, especialmente nas hipóteses de registro de convenção ou de regulamento interno também é necessário apresentar a lista de presença dos condôminos. Nestes casos, a exigência da lista de presença num determinado formato não é mero arbítrio, mas, sim, decorrente do **cumprimento de uma obrigação legal ou regulatória**. Por isso, não é possível desvincular a lista de presença da ata a ser registrada.

Para fins de maior transparência com os condôminos participantes da assembleia, recomenda-se que eles sejam informados da finalidade da lista de presença e o uso que será feito dos dados. Isto pode ser realizado na própria ata, incluindo as informações relevantes sobre seu uso e o tratamento de dados dela decorrentes.

Por outro lado, para assembleias convocadas em virtude de quaisquer outros temas, o registro da lista de presença não é obrigatório. Vale lembrar também que essa lista não é objeto de livre circulação: ao distribuir cópias da ata para ciência dos condôminos, não deve ser incluída cópia da lista de presença como anexo, visto que isso poderia configurar uma divulgação desnecessária e excessiva de dados pessoais.

Para fins de maior transparência com os condôminos participantes da assembleia,

recomenda-se que eles sejam informados da finalidade da lista de presença e o uso que será feito dos dados. Isto pode ser realizado na própria ata, incluindo as informações relevantes sobre seu uso e o tratamento de dados dela decorrentes.

É possível minimizar os dados constantes na lista de presença da assembleia?

Os dados minimamente necessários para formalizar a presença do condômino na lista são: seu nome, sua assinatura, a unidade em que reside, seu CPF, seu telefone e/ou seu e-mail, para finalidade de contato. Destes dados, seria possível suprimir o telefone e o e-mail do condômino quando do registro da lista de presença. Os demais, porém, são necessários para a correta identificação do condômino participante.

Ainda, com a crescente adoção das assembleias mediadas por ferramentas tecnológicas (feitas por vídeo, por exemplo), existem ferramentas que captam os dados do dispositivo de acesso dos participantes, como endereço de IP, modelo do dispositivo, sistema operacional, entre outros. Via de regra, estes dados são necessários para viabilizar o uso da ferramenta, mas não para o registro de presença em si. Por isso, é importante considerar o modo como relatórios de presença são extraídos destas ferramentas, para que sejam aproveitados somente os dados de fato necessários.

Nos casos de procuração de assembleias, quais dados precisam ser informados e constar do documento? Podem fornecer cópia da procuração quando solicitado?

Os dados que devem constar da procuração, caso não estejam expressamente indicados na convenção do condomínio, devem ser suficientes para indicar o condômino que está outorgando poderes e o outorgado, que está recebendo poderes, bem como as informações específicas da assembleia, tais como data, horário de forma de realização. Em geral, espera-se que estas informações sejam verificadas previamente pelo presidente da assembleia ou pelo síndico. Como muitos documentos, essa procuração não deve ser um documento de livre circulação. Quando solicitada, recomenda-se que ela seja enviada para um e-mail ou endereço específico da administradora, a fim de evitar uma divulgação indevida dos dados dos envolvidos.

C. Segurança

Para atividades voltadas à segurança, como sistema de vigilância e portaria, é permitido compartilhar os dados pessoais dos condôminos com empresas terceirizadas?

Sim, é permitido. Sem este compartilhamento o serviço em si seria inviabilizado. Mas, como já mencionamos ao longo deste guia, o compartilhamento deve estar sujeito às regras da LGPD, com medidas de segurança adequadas e a negociação de um contrato que contenha cláusulas adequadas de proteção de dados. Não custa lembrar algumas dicas importantes:

- priorize a contratação de parceiros que estejam em conformidade com a LGPD;
- inclua, no contrato ou em aditivo, cláusulas de proteção de dados que delimitem os deveres e responsabilidades das partes, com especial atenção às medidas de segurança adotadas pelo parceiro contratado;
- informe aos condôminos (titulares de dados) sobre este compartilhamento, incluindo-o no aviso de privacidade do condomínio ou documento semelhante.

O que é importante saber sobre o monitoramento por câmeras nos condomínios?

Além das recomendações gerais mencionadas no Capítulo II (em *O que é importante saber sobre monitoramento por câmeras?*), vale destacar aqui alguns cuidados adicionais:

- **Sobre as pessoas autorizadas a ter acesso às imagens:** a questão sobre este acesso é algo que deve ser definido por cada condomínio, conforme as suas particularidades. Esse ponto não envolve tanto onde estão os monitores por onde as imagens passam (por exemplo, na portaria, visíveis para todos), mas sobretudo aqueles que podem de fato acessar estas imagens para apurar eventuais ocorrências. A depender do caso, pode ser interessante autorizar o síndico, o responsável pela segurança, o zelador, entre outros, para esta

gestão. Para resguardar os direitos de todos, é importante que as pessoas autorizadas assinem um termo de responsabilidade, comprometendo-se a manter a confidencialidade e a segurança das imagens captadas.

- **Pedidos de disponibilização de imagens feitos por condôminos:** em determinadas intercorrências, como acidentes, brigas, ou outros eventos, é comum que os condôminos solicitem o acesso aos registros das câmeras. Nesses casos, é recomendado que uma pessoa autorizada, quando estritamente necessário para o atingimento de uma finalidade lícita, somente mostre as imagens, sem disponibilizá-las, para resguardar sua segurança e confidencialidade. A disponibilização dessas imagens deve ser feita somente em casos específicos, como os aqueles envolvendo investigações ou requisições judiciais.

O que fazer com o registro de visitantes que circulam nos condomínios, especialmente comerciais? Quais dados devem ser solicitados?

O controle de acesso de visitantes provavelmente é uma das atividades do condomínio que lida com **maior volume de dados pessoais** e, justamente por isso, deve priorizar a segurança e a minimização dos dados coletados. A seguir, elencamos práticas úteis para esta atividade:

- **Avaliar quais dados de fato são necessários** para identificar o visitante e liberar seu acesso às dependências do condomínio. Por exemplo: geralmente não é necessário solicitar RG e CPF para fins de identificação — um destes documentos deveria ser o suficiente. Ainda, cuidado com o uso de fotos: guardá-las por tempo indeterminado pode representar um grande risco de manter um dado desatualizado, principalmente para visitantes esporádicos.
- **Considerar outros meios de acesso que não a biometria** (impressão digital ou biometria facial). Estes são exemplos de dados pessoais sensíveis, que exigem cuidados redobrados no seu tratamento, incluindo medidas de segurança reforçadas.
- **Conceber uma política de retenção dos dados**, para evitar o acúmulo de

dados desnecessários. O prazo de guarda desses dados depende de diversos fatores, inclusive determinadas leis municipais e/ou estaduais. De qualquer modo, ao considerar o documento para seu condomínio, não estipule períodos longos demais. Um ponto de partida seria guardar os dados pelo prazo de um ano, contado da data da última visita, mas esse tempo pode ser diferente conforme a natureza do condomínio e a finalidade que se deseja alcançar com esse armazenamento.

Que cuidados devem ser tomados caso o condomínio adote portaria eletrônica?

Assim como para outros prestadores de serviço do condomínio, especialmente os ligados à segurança, a adoção de portaria eletrônica necessita de um olhar atento para o modo como os dados dos condôminos, enquanto titulares de dados, são tratados. Não custa lembrar aqui algumas dicas que mencionamos em outros tópicos:

- priorize a contratação de fornecedores com maior grau de conformidade possível com a LGPD;
- no contrato, inclua cláusula ou aditivo de proteção de dados, detalhando os deveres e responsabilidades do fornecedor da portaria eletrônica;
- verifique as medidas de segurança utilizadas pelo fornecedor, especialmente se envolver o uso de biometria para identificar os condôminos e visitantes: dê prioridade a sistemas e certificações reconhecidos pelo mercado — aqui a opinião de um especialista pode ser de grande ajuda;
- seja transparente com os condôminos e visitantes, disponibilizando um aviso de privacidade com as principais informações sobre a portaria eletrônica.

Existem medidas especiais para o tratamento de imagens de crianças e adolescentes?

O registro de imagens de crianças e adolescentes exige **cuidados redobrados**, já que a LGPD limita bastante as situações em que o seu tratamento é autorizado. Para o tratamento de dados de crianças (ou seja, pessoas com até 12 anos de idade incompletos), é necessário o consentimento específico e em destaque de um dos pais ou representante legal.

Considerando que a LGPD não é a única a tratar de crianças e adolescentes, tendo outras legislações que expressamente disciplinam sobre o cuidado que devemos dispensar a elas, para evitar uma exposição grande da criança ou do adolescente menor de 18 anos incompletos de idade, recomendamos as seguintes boas-práticas, além das mencionadas anteriormente, para registros de imagens em geral:

- sinalizar os locais que são gravados por câmeras de segurança, inclusive indicando que podem capturar imagens de crianças e adolescentes;
- posicionar as câmeras de segurança em locais estratégicos e adequados, de modo a não interferir indevidamente na privacidade da criança ou adolescente (por exemplo, evitar a captura de banheiros, fraldários, vestiários). Neste ponto, recomendamos consultar um especialista em segurança para, se necessário, verificar quais são os locais mais adequados para o posicionamento das câmeras;
- limitar o acesso às imagens somente a pessoas autorizadas (por exemplo, o porteiro, os responsáveis pela segurança, entre outros, limitados ao exercício de suas funções); e
- ser ainda mais rigoroso com o prazo de retenção das imagens de crianças e adolescentes, mantendo apenas pelo período necessário.

Que cuidados devem ser tomados com o Livro de Registro de Ocorrências?

As mesmas medidas recomendadas para o sistema de monitoramento valem para o Livro de Registro de Ocorrências. Independentemente de ser em meio digital ou físico, esse registro também deve ser guardado seguindo medidas de segurança adequadas, que incluam também a possibilidade de registrar e rastrear qualquer mudança nos registros (como atualizações e correções).

Vale ressaltar que **isso não significa manter o Livro de Registro de Ocorrências "escondido" ou proibir o seu acesso**, mas sim dar garantias mínimas de que ele será manuseado com cuidado, para evitar a exposição indevida dos envolvidos nas ocorrências ali registradas.

As **notificações de ocorrências** enviadas com base nas informações/reclamações registradas no livro, quando acompanhadas de imagens, não devem incluir informações sobre pessoas não envolvidas. Por isso, é recomendado **borrar os rostos de pessoas não envolvidas e de crianças**, para que não seja possível identificá-las.

Caso especial: Livros de Registro de Ocorrências Eletrônicos

- Os Livros de Registro de Ocorrências em suporte eletrônico devem seguir as mesmas precauções do suporte físico.
- Antes de iniciar (ou migrar) o Livro para suporte eletrônico, informe-se sobre os arquivos e formatos mais utilizados atualmente. Usar o formato eletrônico inadequado pode expor os condôminos a diversos riscos de segurança da informação.

Idealmente, esses cuidados devem ser observados desde o quanto antes, independentemente de serem livros novos ou já iniciados. É interessante que o síndico e/ou a administradora avaliem o modo como as ocorrências foram registradas até então, a fim de determinar se esse modelo permite um registro adequado dos fatos, ao mesmo tempo que, na medida do possível, garanta o respeito à privacidade dos envolvidos. Se for constatada necessidade de mudança nesse registro, é importante comunicar aos condôminos, a fim de que eles tenham informações atualizadas sobre esse procedimento.

Por fim, lembramos que esses Livros de Registro de Ocorrência lidam com dados pessoais dos condôminos e muitas vezes incluem até mesmo dados pessoais sensíveis ou dados de menores de idade. Por isso, eles devem ser armazenados em local seguro, com controle de acesso, pelo prazo recomendado em lei.

D. Relação entre o condomínio e a administradora

Quando se fala na proteção de dados dos condôminos, quem é o responsável por eles: o síndico ou a administradora do condomínio?

Esta questão tem dois aspectos importantes: por um lado, temos a relação contratual entre o condomínio — na pessoa do síndico — e a administradora; por outro, o poder de tomada de decisão sobre como o tratamento de dados pessoais será realizado.

Sobre a relação contratual em si, temos que a administradora é uma empresa contratada com o objetivo de **exercer funções que a lei permite que sejam delegadas pelo síndico**. Muitas dessas funções — cobranças de pagamentos e dívidas, cotação de seguro, prestação de determinados serviços — dependem do tratamento dos dados pessoais dos moradores e condôminos. Ao realizar essas atividades de tratamento, muitas vezes a administradora atuará como **operadora de dados**, tratando-os em nome do condomínio e agindo conforme as orientações do seu representante. Em outros contextos, a administradora atuará como **controladora** dos dados, especialmente quando goza de certa autonomia ou quando precisa tratá-los para finalidades específicas e por ela definidas.

Toda esta explicação tem como objetivo esclarecer que, no fim, tanto o condomínio, ainda que representado pelo síndico, quanto a administradora têm responsabilidade sobre o tratamento dos dados pessoais dos condôminos. Não obstante, a maior responsabilidade e o dever de fiscalização recaem sobre o condomínio, que pode buscar a responsabilização da empresa contratada, nas hipóteses em que a perda ou dano decorra de sua ação ou omissão dolosa ou culposa.

Como proceder com os dados pessoais dos condôminos e moradores se o contrato com a administradora for rescindido?

Em primeiro lugar, independentemente de questões relacionadas à rescisão, **é fundamental que os condomínios aditem os contratos com as administradoras para incluir cláusulas de proteção de dados**. É por meio delas que serão formalizadas as responsabilidades de cada uma das partes, incluindo a possibilidade de o condomínio exercer maior controle sobre as atividades da administradora.

Para o tema específico da rescisão e de como lidar com os dados pessoais ao término do contrato, é importante que o contrato contenha, no mínimo, as seguintes previsões:

- determinação de que a administradora deverá eliminar todos os dados compartilhados pelo condomínio, com exceção dos que ela seja legalmente obrigada a manter (para o cumprimento de obrigações legais ou regulatórias); e
- obrigação de a administradora adotar os meios técnicos adequados para permitir que as informações até então tratadas sejam compatíveis com o sistema adotado por nova empresa eventualmente contratada pelo condomínio ao término do contrato.

E. Cuidados sanitários

Em caso de epidemias ou surtos de doenças infectocontagiosas no condomínio, que cuidados devem ser adotados com a informação aos condôminos e o tratamento de seus dados pessoais?

Recentemente, com a pandemia de Covid-19, muitos condomínios se viram obrigados a adotar protocolos e medidas sanitárias a fim de garantir a segurança dos moradores e condôminos. Quando o assunto é **saúde e dados pessoais**, devemos ser cautelosos, pois estamos diante de **dados pessoais sensíveis**, que apresentam um alto risco de discriminação dos titulares se utilizados indevidamente. Por isso, é importante que as informações relevantes para garantir a **segurança e bem-estar** dos condôminos **não os exponham indevidamente**.

Com isso em mente, recomendamos que o condomínio considere algumas das medidas que elencamos a seguir:

- incentive os condôminos a procurarem a vacinação disponível;
- crie um canal de comunicação específico para assuntos relacionados à pandemia (que pode ser reaproveitado em caso de outros surtos de doenças infectocontagiosas no condomínio);
- solicite que os condôminos que desenvolverem sintomas de Covid-19 (ou de outra doença preocupante) se utilizem desse canal para notificar o condomínio;
- incentive também que condôminos que tiveram contato com pessoas doentes (como visitantes, prestadores de serviço) também notifiquem esta informação;
- restrinja o acesso a estas notificações a somente as pessoas realmente necessárias (síndico, administrador, entre outros que o condomínio considerar indispensáveis);
- ao divulgar informativos sobre possíveis casos no condomínio, informe somente os dados necessários para que os condôminos possam se proteger, mas sem expor a identidade do doente (mencionar a torre ou andar em que o caso foi identificado).

Ressaltamos que essas medidas são importantes para os tempos de pandemia, mas também podem ser mantidas sempre que for localizado algum surto de doença infectocontagiosa no condomínio (sarampo, dengue, gripe, entre outras). Cuidar da saúde e proteger a privacidade é um dever de todos!



CAPÍTULO VII

COMPARTILHAMENTO DE DADOS E RELAÇÃO ENTRE OS PLAYERS DO MERCADO IMOBILIÁRIO



Sendo um mercado com relação muito forte com as pessoas em geral, o mercado imobiliário depende também do tratamento de dados pessoais de pessoas em diversas posições — sejam eles investidores, colaboradores de empresas, prestadores de serviço, condôminos, locadores ou locatários, proprietários de imóveis, entre tantos outros. Nos capítulos anteriores, abordamos os aspectos específicos de cada uma das atividades. Agora, o objetivo é apresentar os aspectos relacionados ao compartilhamento de dados entre esses diversos agentes, incluindo as maneiras mais adequadas de viabilizar esse compartilhamento e dicas de como torná-lo mais seguro.

A. Preparando o terreno: bases legais e a expectativa do titular de dados

Todo compartilhamento de dados precisa ser justificado por uma base legal adequada. Como vimos nos conceitos básicos, o tratamento nem sempre precisa do consentimento do titular de dados. Às vezes, o tratamento é decorrente do cumprimento de uma obrigação legal, de um contrato celebrado entre as partes ou, ainda, faz parte dos interesses legítimos do controlador em promover seu negócio. Por isso, aqui vão algumas recomendações gerais de como “preparar o terreno” e comunicar aos titulares sobre o compartilhamento.

- **Tenha um aviso de privacidade (ou política de privacidade).** Como comentamos acima, esse documento é essencial, pois comunica de forma fácil aos titulares de dados as principais características do tratamento de dados, incluindo a possibilidade de compartilhamento. Não é necessário listar nominalmente todas as empresas com quem os dados do titular são compartilhados, mas é recomendado no mínimo dispor suas categorias (parceiros comerciais, provedores de infraestrutura técnica, membros do mesmo grupo empresarial etc.).
- **No caso de cumprimento de obrigação legal ou regulatória.** Se o compartilhamento é previsto na lei (por exemplo, para viabilizar a regulamentação do edifício), então não há como se opor a este compartilhamento. Como boa prática, a empresa deve destacar essa possibilidade de compartilhamento no seu aviso de privacidade.

- **No caso da execução de contrato com o titular.** Informe o titular, se possível no próprio contrato, que seus dados serão compartilhados para permitir o cumprimento daquele contrato e dê exemplos de finalidades em que isso será necessário (por exemplo, para avaliar o crédito do titular ou uma proposta de locação). Lembrando que esta base legal vale tanto para os procedimentos preliminares ao contrato quanto para a execução do contrato em si.
- **No caso do legítimo interesse.** Utilize sempre estratégias de comunicação que criem no titular a expectativa de ter seu dado tratado e compartilhado com outras empresas e que esse compartilhamento pode ser do seu interesse. Para mais informações veja o item de prospecção de clientes no Capítulo IV.

B. Compartilhamentos necessários no decorrer dos negócios

Transferências de administradoras de condomínio

Como responsáveis por uma série de obrigações essenciais do condomínio (incluindo as cobranças de pagamentos e de multas), o tratamento de dados pessoais é uma das mais importantes atividades do negócio das administradoras. Por isso, ao negociar a contratação ou a transição de uma administradora para a outra, fique atento ao seguinte:

- **Conformidade à LGPD e medidas de segurança adequadas.** A conformidade da empresa à LGPD agora deve ser um critério determinante. Procure saber informações sobre as medidas que a empresa utilizou para se adequar à LGPD e quais benefícios a administradora pode trazer ao condomínio.
- **Utilização de sistemas e/ou arquivos interoperáveis.** Para evitar a incompatibilidade entre os sistemas ou os tipos de arquivos utilizados pelas empresas, especifique no contrato que, pelo menos em caso de transição, a empresa deverá apresentar os arquivos em formatos interoperáveis, ou seja, que são aceitos por diversos programas.

- **Obrigação de eliminação dos dados ao término do contrato.** A menos que a contratada seja legalmente obrigada a reter certos dados por um período determinado, é altamente recomendável que o contrato preveja a obrigação da contratada de excluir estes dados ao final do contrato.

Compartilhamento de documentos e outros dados obrigatórios para regularização do ativo imobiliário

Desde o processo de incorporação, até a construção e a instalação do condomínio, as leis brasileiras exigem uma série de documentos de indivíduos relacionados ao empreendimento, inclusive, em certo ponto, dos futuros moradores. Nesse sentido, tenha especial cuidado com a segurança do armazenamento desses documentos e dos seus prazos de retenção, a fim de evitar incidentes de segurança e a exposição indevida dos dados (lembrando que a LGPD se aplica também para os dados tratados em meios físicos, não só nos digitais).

Compartilhamento de dados entre incorporadora e empresa responsável pelo lançamento do empreendimento

As parcerias com empresas de lançamentos podem ajudar muito na divulgação do novo empreendimento. Mas, como tudo envolvendo dados pessoais, esse compartilhamento de dados deve ser feito com cautela, para evitar que os dados sejam utilizados para finalidades não relacionadas e que exponham os titulares a riscos desnecessários. Por isso, vale relembrar aqui algumas dicas que mencionamos em outros assuntos deste guia:

- sempre formalize este compartilhamento em um contrato — ou aditivo — com cláusula específica de proteção de dados;
- na cláusula, inclua previsões sobre as responsabilidades de cada uma das partes, limitando a finalidade de uso dos dados e priorizando medidas de segurança adequadas;

- contrate empresas que demonstrem estar adequadas à LGPD;
- Para mais detalhes, recomendamos consultar as recomendações no Capítulo IV, sobre a atividade de intermediação de vendas e locação.

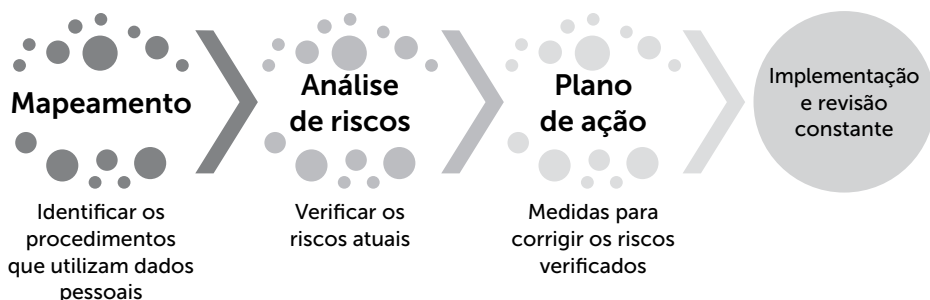


CAPÍTULO VIII

O PROCESSO DE ADEQUAÇÃO À LGPD NA PRÁTICA



Como em muitas situações que exigem ações de melhoria, o processo de adequação à LGPD passa por basicamente quatro etapas:



Uma vez realizado o mapeamento e verificados quais os riscos envolvidos em cada atividade de tratamento executada pela empresa ou pelo condomínio, deverá ser definido um Plano de Ação para eliminá-los ou minimizá-los, conforme o caso.

A. Medidas do Plano de Ação

Registro e mapeamento dos dados

O primeiro passo é registrar e mapear os dados pessoais tratados. Esse mapeamento deve conter:

- a categorização dos dados pessoais — se são dados pessoais, dados pessoais sensíveis ou dados de crianças ou outro dado que possa representar um risco maior de tratamento;
- a categorização dos titulares — se são clientes, colaboradores, investidores, administradores, se são menores de idade etc.;
- as bases legais utilizadas em cada atividade de tratamento;
- as medidas de transparência utilizadas com o titular — se estão num aviso de privacidade, no contrato ou outro meio semelhante;

- o prazo de conservação dos dados, conforme uma política de retenção de dados ou uma tabela de temporalidade;
- o fluxo dos dados — como ele é obtido, para que é utilizado, onde fica armazenado e como é descartado;
- as medidas de segurança utilizadas.

Nomeação de um Encarregado pela Proteção de Dados Pessoais (DPO)

Principalmente no caso das empresas, a nomeação do Encarregado mostra um comprometimento com a LGPD e auxiliará no seu processo de adequação e no relacionamento com a Autoridade Nacional de Proteção de Dados e os titulares. Para os condomínios, a nomeação de um DPO também é altamente recomendável; porém, diretrizes mais detalhadas sobre a obrigatoriedade do DPO serão emitidas pela ANPD muito provavelmente em 2022.

Criar políticas e procedimentos

As empresas e condomínios devem criar políticas e procedimentos para viabilizar o cumprimento das normas de proteção de dados e para reforçar o projeto de adequação à LGPD. Documentos importantes são:

- Avisos e Privacidade — interno para os colaboradores; externo para os clientes e terceiros;
- Política de Manuseio de Dados Pessoais;
- Política Institucional de Privacidade;
- Procedimentos relacionados às Respostas a Requisições de Órgãos Públicos;
- Procedimentos para respostas às requisições dos Titulares de Dados;

- Procedimentos para o uso compartilhado de Dados Pessoais;
- Procedimento de Resposta a Incidentes de Segurança.

Divulgar normas, políticas e procedimentos e realizar treinamentos

Todas as normas de proteção de dados devem ser divulgadas a todos os colaboradores da empresa e do condomínio, independentemente do seu nível hierárquico. Essa divulgação pode ser reforçada com treinamentos específicos e capacitação dos profissionais que estarão em contato mais direto com o tratamento de dados pessoais.

Criar canal de comunicação com o titular e divulgá-lo amplamente

Criar um canal de comunicação para possibilitar que, de maneira facilitada e ágil, seja possível ao titular de dados promover requisições a respeito de seus dados pessoais e exercer seus direitos. Uma vez criado este canal de comunicação, ele deve ser amplamente divulgado em locais de alta visibilidade. No caso das empresas, essas divulgações devem ocorrer principalmente em seu site e em murais de aviso. No caso dos condomínios, o canal deve ser divulgado aos condôminos e moradores e também exposto em locais visíveis, como murais de aviso nas áreas comuns.

Revisar e aditar contratos

Também é fundamental revisar os contratos existentes a fim de aditá-los para estabelecer obrigações e definir responsabilidades das partes contratantes em termos de tratamento de dados pessoais. Apenas lembrando, sempre considere o seguinte no processo de revisão dos contratos:

- **O fornecedor ou prestador de serviço está adequado à LGPD?** Sempre dê preferência a parceiros que estejam adequados (ou que no mínimo comprovem que estão conduzindo um programa eficiente de adequação à lei).

- **Quem é quem?** Deixe bem claro quem é quem na relação contratual: quem é (são) o(s) controlador(es) e o operador e em relação a quais atividades de tratamento. Em caso de dúvidas, não deixe de consultar um especialista.
- **Há cláusula de sigilo/confidencialidade?** Todas as informações trocadas no decorrer da relação contratual devem ser protegidas pela obrigação de confidencialidade — o que inclui tanto os dados pessoais quanto outras informações relevantes para a prestação dos serviços.
- **Quem vai pagar por isso?** Estar adequado à LGPD é uma obrigação de cada uma das empresas (ou, de maneira mais ampla, pessoas físicas e jurídicas) que realizam tratamento de dados pessoais. Por isso, via de regra, eventuais custos adicionais decorrentes do processo de adequação não devem ser arcados pela outra parte. Recomendamos que este ponto seja negociado entre as partes e formalizado no contrato, para evitar cobranças posteriores pelas medidas adotadas pelo contratado.
- **Como será o gerenciamento dos dados ao final do contrato?** A critério do controlador, ao final do contrato, os dados pessoais devem ser eliminados, devolvidos ou, de alguma forma, inutilizados, para que o prestador não tenha mais acesso a eles. Caso o prestador tenha uma obrigação legal de conservá-los por mais tempo, é importante que o contrato defina que todas as obrigações contidas nele quanto ao tratamento de dados pessoais devem permanecer exigíveis mesmo após o final do contrato, enquanto os dados pessoais forem tratados, nos termos da LGPD.

