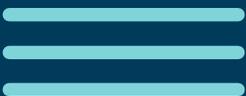


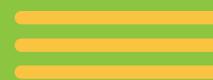
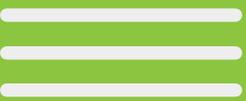
Guia Boas Práticas e Governança em Proteção de Dados Pessoais na Incorporação Imobiliária



ABRAIN
ASSOCIAÇÃO BRASILEIRA DE
INCORPORADORAS IMOBILIÁRIAS

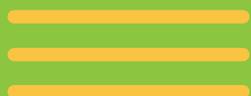
Agosto de 2020





ABRAINC

ASSOCIAÇÃO BRASILEIRA DE
INCORPORADORAS IMOBILIÁRIAS



ÍNDICE

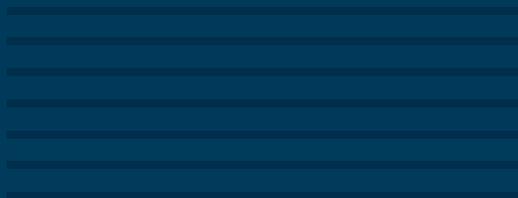
Apresentação	05
O mercado de incorporação e a importância dos dados	06
Contexto de legislações de proteção de dados.....	08
Aplicação da LGPD.....	10

PARTE I ¹³

1. Proteção de dados no mercado de incorporação.....	14
1.1. Captação de clientes.....	15
1.2. Estande de vendas.....	20
1.3. Confeção de contrato e análise de crédito.....	22
1.4. Pós-venda.....	24
2. Proteção de dados de colaboradores.....	25
2.1. Recrutamento e seleção.....	26
2.2. Admissão.....	29
2.3. Monitoramento de empregados.....	30
2.4. Desligamento e arquivamento.....	32
3. Fornecedores, parceiros e terceiros em geral.....	33
3.1. Vendedores de terrenos.....	35
4. Governança de privacidade.....	37
4.1. Boas práticas de organização e funcionamento.....	38
4.2. Políticas.....	39
4.3. Ações educativas e mecanismos internos de supervisão.....	41

PARTE II ⁴²

5. Conceitos	43	10. Encarregado (DPO)	86
6. Princípios	46	11. Segurança da Informação	89
7. Bases legais	52	11.1. Normas técnicas e padrões de segurança	90
7.1. Bases legais para Dados Pessoais	53	11.2. Incidentes	92
7.1.1. Legítimo interesse	56	12. Supervisão, responsabilização e sanções	93
7.1.2. Consentimento	60	12.1. ANPD	94
7.2. Bases legais para Dados Sensíveis	63	12.2. Procon, Senacon e Ministério Público	95
7.2.1. Garantia da prevenção à fraude e à segurança do titular.....	65	12.3. Contencioso em proteção de dados	95
8. Direitos dos titulares	66	13. Checklist de adequação	96
8.1 Exercício de direitos por titulares	73		
8.1.1. Atendimento a petições e reclamações de titulares	74		
9. Obrigações impostas aos agentes de tratamento	76		
9.1. Registro das Atividades de Tratamento	77		
9.2. Padrões de segurança	79		
9.3. Privacy by Design	80		
9.4. Transferências internacionais	81		



Apresentação

O Brasil, seguindo uma tendência mundial de regulação do uso de dados pessoais, aprovou em agosto de 2018 a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). Essa lei impacta todos os setores da economia, incluindo o setor público, exigindo que organizações revisem suas práticas e adaptem seus processos.

A LGPD estabelece conceitos, princípios, direitos dos titulares, requisitos para tratamento de dados pessoais, medidas para realização de transferências internacionais, responsabilidades dos agentes de tratamento de dados e penalidades aplicáveis. Essa lei deve ser interpretada no contexto de atuação de cada empresa e este Guia de Boas Práticas e Governança em Proteção de Dados Pessoais – que chamaremos de Guia – é um guia para todas as incorporadoras que buscam sua adequação.

Busca-se apresentar aqui diretrizes gerais sobre a LGPD, considerando as peculiaridades do mercado de incorporação e avaliando parâmetros para adequação do setor. Ainda que não possa ser considerado uma opinião legal, este documento deve ser analisado pelas incorporadoras como um guia para reafirmar o compromisso do setor com a privacidade e a proteção de dados de seus consumidores, fornecedores e colaboradores.



O mercado de incorporação e a importância dos dados



O tratamento de dados pessoais em uma empresa geralmente contempla duas frentes:

- (i) atividades core da empresa e todo o necessário para divulgar e entregar seus produtos; e
- (ii) as atividades internas, que envolvem dados de colaboradores, fornecedores, parceiros, sócios e administradores.

O mercado de incorporação diferencia-se nessas duas frentes em razão da sua alta integração com terceiros.

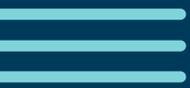
Em relação a seus clientes e potenciais clientes (prospects), as incorporadoras contam com o auxílio de corretores de imóveis¹ e imobiliárias, que atuam na intermediação da compra, venda, permuta e locação de imóveis. Para que essa intermediação possa ocorrer, faz-se necessário o compartilhamen-

to de dados pessoais de clientes e prospects entre a incorporadora – proprietária do imóvel – e corretores ou imobiliárias, que contam com o conhecimento de mercado para encontrar os compradores adequados para cada unidade.

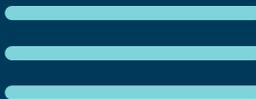
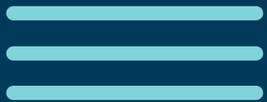
Efetuada a compra, caso o imóvel seja financiado, há o compartilhamento de dados com as instituições financeiras e, quando iniciada a cobrança da taxa condominial, pode haver também o compartilhamento dos dados com as administradoras de condomínio.

Do outro lado do negócio, para viabilizar a construção dos imóveis, as incorporadoras também dependem de compartilhamento de dados com sociedades do grupo (especialmente Sociedades de Propósito Específico – SPE, constituídas para cada imóvel) ou com construtoras. Por fim, nada disso seria possível sem os colaboradores e fornecedores que atuam para que toda a cadeia funcione.

¹Lei nº 6.530/1978, art. 3º.



Contexto de legislações de proteção de dados



A LGPD está inserida num contexto internacional de legislações que tratam de proteção de dados pessoais. Nacionalmente, a lei também integra um conjunto de outras regulações que dispõem sobre privacidade e proteção de dados pessoais no Brasil.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou nos anos 1980 as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, que influenciou as regulações de diversos países sobre o tema. No cenário internacional, verifica-se na última década a aprovação ou alteração de regras de proteção de dados pessoais em diversos países e mercados, como México², Colômbia³, Singapura⁴, algumas unidades federativas dos Estados Unidos da América, além do Espaço Econômico Europeu⁵.

No Brasil, o direito à intimidade e vida privada é disposto na Constituição Federal e há dispositivos de proteção de dados pessoais em diferentes regulações: Código de Defesa do Consumidor, Marco Civil da Internet, Lei do Cadastro Positivo, Lei do Sigilo Bancário, entre outras. A LGPD não revoga expressamente nenhuma dessas regras, sendo que uma de suas principais contribuições é nortear a interpretação das diferentes leis e unificar conceitos.

² Ley Federal de Protección de Datos Personales em Posesión de los Particulares de 2010

³ Ley 1581/2012

⁴ Personal Data Protection Act 2012

⁵ Regulamento 2016/679 – GDPR

Aplicação da LGPD



A LGPD se aplica a todas as atividades de tratamento de dados pessoais **(i)** realizadas no Brasil; **(ii)** com dados coletados no Brasil; ou **(iii)** realizadas por empresas que busquem oferecer ou fornecer bens ou serviços no Brasil. Note que esses requisitos não são cumulativos e o atendimento a um deles é suficiente para que a LGPD tenha que ser respeitada.

Trata-se de uma regra com ampla aplicabilidade. O tratamento de dados pessoais envolve qualquer operação realizada com o dado pessoal, como o armazenamento, o acesso, o compartilhamento e até a exclusão. Dado pessoal é qualquer dado que pode levar à identificação de uma pessoa: aqui podem ser incluídos nome, foto, endereço de e-mail corporativo, número de telefone, hábitos de navegação, números identificadores de clientes ou colaboradores e qualquer outro dado que sirva para individualizar uma pessoa física.

Não se aplica a LGPD para:

- a)** dados que identifiquem pessoas jurídicas (como razão social e CNPJ);
- b)** dados anonimizados – que não permitem a identificação das pessoas;
- c)** atividades de tratamento realizadas para fins exclusivamente particulares e não econômicos;
- d)** atividades de tratamento com fins jornalísticos e artísticos;
- e)** atividades de tratamento com fins acadêmicos; e
- f)** atividades de tratamento realizadas pelo poder público ou por entidade privada agindo em nome do poder público com fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.





Para entender como a LGPD se aplica na prática ao mercado de incorporação, este guia se divide em duas partes: na primeira, avaliam-se os principais processos de tratamento de dados numa incorporadora e, na segunda, apresentam-se os principais conceitos legais.





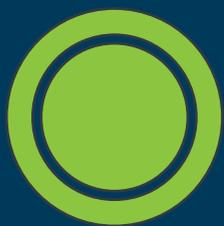
PARTE I

Esta primeira parte busca oferecer diretrizes práticas a serem aplicadas às principais atividades de negócio das incorporadoras, iniciando pelos dados dos clientes e, em seguida, avaliando relações com colaboradores e fornecedores. Finalizando esta primeira sessão, consta uma análise de aspectos de governança em proteção de dados.



1

Proteção de dados no mercado de incorporação



Todos os conceitos, princípios, bases legais, direitos e demais requisitos legais devem ser aplicados a cada atividade de tratamento de dados pessoais da incorporadora – caso tenha qualquer dúvida, consulte a Parte 2 deste Guia para melhor entender os conceitos.

1.1. Captação de clientes

O contato da incorporadora com possíveis clientes pode se dar por iniciativa do próprio titular ou por campanhas e análise de dados das incorporadoras. No primeiro caso, podemos mencionar as variadas formas de contato disponíveis, de contato telefônico à disponibilização e uma plataforma de chat online com corretor.

No segundo, campanhas de marketing digital, como anúncios impulsionados em redes sociais, postagens em blogs e páginas oficiais da incorporadora, além de enriquecimento de base de dados com dados de terceiros (third-party data) devem observar certas diretrizes.

/ Contato pelo site, telefone, e-mail ou chat

A incorporadora deve verificar quais dados serão necessários coletar, onde eles serão armazenados e como o titular pode receber informações sobre a política de privacidade da incorporadora. Uma possibilidade é instruir os atendentes a indicar onde encontrar a política de privacidade da empresa no site, por exemplo, ou, em caso de contato por escrito, disponibilizar um aviso de privacidade no momento da coleta dos dados.

Caso a pessoa responsável por atender o prospect seja um terceiro – como um corretor ou um atendente terceirizado – a incorporadora deve considerar firmar com esses indivíduos termos específicos de proteção de dados e confidencialidade. Além disso, por serem terceiros não subordinados à incorporadora, a empresa pode adotar técnicas de pseudonimização ao compartilhar esses dados ou minimizar os dados que serão compartilhados.

Especificamente em relação aos formulários de contato, é importante que os formulários colem apenas os dados estritamente necessários, deixem clara a finalidade de coleta de cada dado e tenham link para a política de privacidade da incorporadora, além de avisos de privacidade, se necessário.

Quanto aos chats, as plataformas costumam ser operadas por empresas terceiras e a incorporadora deve certificar-se se essas empresas têm acesso aos dados e se nos contratos há disposições específicas de proteção de dados.

Além disso, a incorporadora deve fornecer ao titular informações suficientes sobre o tratamento dos dados pessoais. Enumeramos abaixo possíveis mensagens para incluir em cada uma dessas situações:

Telefone:

Para atendê-lo, precisamos coletar alguns dados seus. Esses dados poderão ser compartilhados com imobiliárias parceiras e corretores, caso queira receber informações sobre nossos empreendimentos. Para entender melhor como a *[nome da incorporadora]* trata seus dados pessoais, acesse nossa Política de Privacidade em nosso site *[www.nomedaincorporadora.com.br]* ou entre em contato com nosso encarregado *[contato do Encarregado]*.

Respostas de e-mail:

Você está recebendo este e-mail por ter entrado em contato com a *[nome da incorporadora]* por e-mail. Caso não tenha sido você, por favor informe-nos clicando aqui e ignore este e-mail. Os dados pessoais que você nos enviar poderão ser compartilhados com imobiliárias parceiras e corretores, caso queira receber informações sobre nossos empreendimentos. Para entender melhor como a *[nome da incorporadora]* trata seus dados pessoais, acesse nossa Política de Privacidade ou entre em contato com nosso encarregado *[contato do Encarregado]*.

Formulário de contato e chat:

Os dados informados neste formulário serão utilizados para que possamos entrar em contato com você, conforme solicitado. Nosso atendimento é realizado por imobiliárias parceiras e corretores, que se comprometem a proteger sua privacidade e seus dados pessoais. Para entender melhor como a *[nome da incorporadora]* trata seus dados pessoais, acesse nossa Política de Privacidade ou entre em contato com nosso encarregado *[contato do Encarregado]*.

No caso dos formulários, a incorporadora também pode utilizar **just-in-time notices**, que são avisos curtos que aparecem quando o titular clica no campo a ser preenchido, indicando a finalidade do tratamento, conforme exemplo a seguir:

Dados Pessoais

Nome completo:

Telefone:

Pedimos seu telefone para entrar em contato com você sobre nossos empreendimentos

/ Na prática

/ Com os dados recebidos ou coletados diretamente do prospect, a incorporadora poderá **(i)** responder a demanda do prospect; **(ii)** cadastrar o prospect em sua base de dados, conforme interesse demonstrado na mensagem; **(iii)** enviar novas mensagens relacionadas a esse interesse, exceto se o titular se opor ao seu recebimento.

/ O formulário de contato do site deve perguntar como o prospect prefere ser contatado (telefone, e-mail, mensagens de texto etc.) e, a partir da resposta, requerer apenas o dado necessário para realizar aquele contato.

! Caso a incorporadora precise compartilhar esses dados com terceiros, como imobiliárias ou corretores, a empresa deve **(i)** verificar quais dados precisam ser compartilhados para o atendimento; **(ii)** certificar-se de que os terceiros não utilizarão os dados para outras finalidades; **(iii)** avaliar a possibilidade de pseudonimizar os dados antes do compartilhamento. Podem ser adotadas tecnologias de mascaramento de dados pessoais, especialmente números de telefone, permitindo que o corretor entre em contato sem ter acesso ao número de telefone⁶ do prospect.

/ Marketing digital

A LGPD não proíbe a realização de marketing digital. Pelo contrário: a base legal do legítimo interesse pode ser uma forte aliada das empresas no momento da captação de novos negócios. O uso indevido de dados, como a aquisição de mailings de fonte desconhecida e sem base legal adequada, já é ilegal⁷ e continuará vedado pela legislação. As incorporadoras devem adotar uma postura proativa para minimizar o uso de dados de fontes não confiáveis ou que não tenham rastreabilidade, além de trabalharem na conscientização dos terceiros que acessam suas bases de dados.

A incorporadora deve verificar se utiliza serviços de terceiros – como agências – para auxiliar no desenvolvimento da estratégia e operacionalizar suas campanhas digitais. Caso positivo, é preciso averiguar se há compartilhamento de dados de prospects ou clientes com a agência e como esse compartilhamento ocorre. Mais uma vez, técnicas de pseudonimização podem ser adotadas para minimizar o risco do compartilhamento, além da adoção de cláusulas contratuais específicas.

Na hipótese de a incorporadora adquirir base de dados de terceiros ou realizar o enriquecimento de sua base de dados com dados de terceiros, a incorporadora deve certificar-se de que o terceiro está adequado à legislação e que tem uma base legal válida para

realizar suas atividades. Essas condições também devem ser refletidas contratualmente.

Caso a incorporadora permita que terceiros, como corretores, alimentem o software de gestão de relacionamento com o cliente (CRM), sugerimos adotar as seguintes medidas para mitigar riscos:

- (i)** Incluir um campo para o corretor inserir a fonte do dado (ex.: visitante do estande; chat online; contato pessoal; base de dados de terceiro). Caso seja base de dados de terceiro, indicar qual o terceiro;
- (ii)** Inserir um aviso lembrando o corretor sobre a necessidade de cumprir com as regras de proteção de dados e que contatos advindos de fontes ilícitas ou inadequadas serão removidos; e
- (iii)** Em casos potencialmente ilícitos (ex.: inserção cuja fonte é base de dados de terceiro não identificado), pedir maiores detalhes ao corretor ou excluir o dado.

⁷A título exemplificativo, cita-se o artigo 43 do Código de Defesa do Consumidor e o artigo 7º, VII do Marco Civil da Internet.

1.2. Estande de vendas

O estande de vendas é um importante ponto de contato da incorporadora com o público. De forma similar ao que ocorre no contato digital, há terceiros envolvidos nas atividades de tratamento de dados pessoais, desde a recepção e cadastro do prospect até eventual confecção de contrato e análise de crédito.

De forma geral, é comum as incorporadoras

- (i) contratarem recepcionistas terceirizados, que ficam responsáveis por coletar os dados iniciais do cliente para direcioná-lo ao corretor;
- (ii) contarem com corretores terceirizados ou imobiliárias parceiras para realização do atendimento no estande; e
- (iii) tenham parceiros para realizar análise de crédito e confeccionar contratos.

/ Na prática

De forma a ter um nível mínimo de adequação, sugere-se que as incorporadoras:

- (i) Treinem o responsável pela coleta dos dados para explicar ao titular como ele pode acessar informações sobre o tratamento de seus dados pessoais. A incorporadora pode, por exemplo, ter uma cópia física e um QR code para que o cliente possa acessar a política de privacidade do seu celular;
- (ii) Reforcem junto aos terceiros a importância de manter os dados em sigilo e que o compartilhamento com pessoas não autorizadas pode ensejar responsabilidades;
- (iii) Firmem um termo de sigilo e proteção de dados com os terceiros que trabalham no estande; e
- (iv) Caso o titular tenha informado e-mail ou telefone, enviem a Política de Privacidade e os canais para exercício de direitos, o que também deve estar disponível para consulta no local.

Caso a incorporadora queira melhorar seus controles e nível de proteção e dados, além das medidas acima, sugere-se a adoção das seguintes práticas:

(i) Disponibilizar terminais de autoatendimento nos estandes, permitindo que o titular realize seu cadastro, com nenhum ou pouco auxílio de terceiros; e

(ii) Limitar o acesso dos terceiros – inclusive corretores – aos dados, conforme a necessidade de atendimento. Exemplificativamente, para atendimento no local, o corretor teria acesso ao nome do titular, mas não ao e-mail ou telefone, o que seria fornecido apenas se o Titular assim concordar. Essa concordância poderá ser posterior ao atendimento, por meio de questionamento no local, por SMS ou e-mail.

1.3. Confecção de contrato e análise de crédito

Caso o prospect decida adquirir uma unidade da incorporadora, mais dados serão necessários para formalizar o negócio. Legalmente, diversos dados são necessários para elaborar o contrato, realizar a análise de crédito, possibilitar o financiamento e, futuramente, firmar a escritura de compra e venda. Para endereçar esses aspectos, recomenda-se a inclusão de uma cláusula de proteção de dados nos contratos padrão, conforme exemplo ao lado.

Nessa etapa de fechamento do negócio, é comum que a incorporadora faça cópias de documentos, peça para que o cliente preencha formulários, forneça certidões e comprovantes de renda, entre outros. Além disso, é possível que terceiros elaborem os contratos.

O Comprador recebeu e está ciente da Política de Privacidade da [incorporadora], cujas cláusulas fazem parte deste contrato. O Comprador compreende que, para a regular execução deste Contrato, a [incorporadora] tratará dados pessoais do Comprador, tais como dados de identificação (como nome completo, estado civil, profissão, RG, CPF) e dados relativos a endereço de residência, além de dados referentes a renda. Os dados são necessários para a execução do objeto do Contrato ou para atender a interesses legítimos da [incorporadora], sempre que estes não se sobrepuserem aos direitos garantidos ao Comprador.

§ 1º A [incorporadora] se compromete a tratar os Dados Pessoais do Comprador de acordo com a política de privacidade disponibilizada. Ainda, quando houver necessidade, a [incorporadora] poderá compartilhar os dados pessoais com seus fornecedores, parceiros órgãos da Administração Pública ou terceiros autorizados para que a [incorporadora] ou tais terceiros possam resguardar seus direitos em relação às obrigações aplicáveis.

§ 2º Caso o comprador tenha qualquer dúvida em relação ao tratamento de seus Dados Pessoais pela [incorporadora] ou queira requerer o exercício de qualquer direito, este poderá utilizar os canais disponíveis para tanto, nos termos da Política de Privacidade.

/ Na prática

De forma a ter um nível mínimo de adequação, sugere-se que as incorporadoras:

- (i)** Verifiquem se são necessárias cópias de documentos além dos dados inseridos nos formulários e, em caso positivo, armazenem-nas em local seguro;
- (ii)** Instruam terceiros que recebam estes documentos a armazená-los no local correto e excluam cópias eventualmente recebidas por e-mail ou celular;
- (iii)** Informem o titular sobre a existência de decisões automatizadas, se houver, especialmente relativas à análise de crédito;
- (iv)** Tenham cláusulas contratuais específicas de proteção de dados no contrato de compra e venda e com os terceiros que acessam os dados pessoais;
- (v)** Forneçam de forma facilitada informações sobre os terceiros com quem a incorporadora irá compartilhar os dados, tais como instituições financeiras, securitizadoras, gestoras de condomínio e seguradoras; e
- (vi)** Reforcem junto aos terceiros a importância de manter os dados em sigilo, destacando que o compartilhamento com pessoas não autorizadas pode ensejar responsabilidades.

Caso a incorporadora queira melhorar seus controles e nível de proteção e dados, além das medidas acima, sugere-se a adoção das seguintes práticas:

- (i)** Implementar tecnologia para recebimento de documentos, em que o próprio cliente pode realizar o upload dos documentos necessários, sem necessidade de enviá-los por e-mail; e
- (ii)** Criar uma central de privacidade para os clientes, que poderão acessar seus dados pessoais, retificá-los e verificar os terceiros com quem os dados foram compartilhados. Essa central pode ser uma funcionalidade do portal do cliente, caso exista.

Concluída a venda, o prospect passa a ser um cliente e outras atividades de tratamento de dados se iniciam, como cobrança, entrega de chaves, lavratura da escritura e assistência técnica. Nesse ponto, o contato do cliente passa a ser com a área de relacionamento com o cliente da incorporadora e vê-se a diminuição do contato com o corretor de imóveis. Por outro lado, vislumbram-se novos terceiros na cadeia, como instituições financeiras, administradoras de condomínio, empresas que realizam reparos e assistência técnica, entre outros.

1.4. Pós-venda

/ Na prática

De forma a ter um nível mínimo de adequação, sugere-se que incorporadoras:

(i) Informem aos clientes eventuais transferências de dados pessoais a terceiros (como empresas de cobrança e administradoras de condomínio);

(ii) Averiguem o nível de conformidade com os terceiros;

(iii) Reforcem junto aos terceiros a importância de manter os dados em sigilo, destacando que o compartilhamento com pessoas não autorizadas pode ensejar responsabilidades; e

(iv) Firmem um termo de sigilo e proteção de dados com os terceiros que acessem dados pessoais de clientes.



2

Proteção de dados de colaboradores



Os colaboradores são peças-chave para o sucesso do programa de governança em proteção de dados da empresa. Ao mesmo tempo em que atuarão diretamente nos processos de tratamento de dados pessoais, são titulares de dados pessoais tratados pela incorporadora.

Para que o tema de privacidade seja seriamente tratado pelos colaboradores, a incorporadora deve demonstrar que essa preocupação não se dá apenas em relação aos clientes. O cuidado da incorporadora com os dados de seus colaboradores deve se dar desde o processo de recrutamento e seleção até o desligamento do colaborador.

2.1. Recrutamento e seleção

Ao abrir uma nova oportunidade de trabalho em seu quadro, a incorporadora pode (i) receber currículos enviados pelos próprios candidatos; (ii) contratar uma agência de recrutamento para realizar este trabalho; ou (iii) buscar profissionais no mercado usando plataformas próprias para isso (como LinkedIn). É possível interpretar que os currículos enviados pelos próprios candidatos à incorporadora constituem consentimento do candidato para o tratamento de dados realizado no âmbito do processo seletivo. Nos demais casos, a incorporadora poderá valer-se de seu legítimo interesse.

/ Na prática

Em relação ao processo de recrutamento, destacamos os seguintes pontos de atenção em relação à proteção de dados:

- (i)** Incluir na Política de Privacidade da incorporadora questões específicas relacionadas ao tratamento de dados de candidatos a emprego ou criar uma política específica para tanto;
- (ii)** Incluir nos textos de descrição das vagas avisos específicos de privacidade, conforme sugestão abaixo, o qual deverá ser revisado considerando o caso concreto:

Ao enviar seus dados pessoais para participação no processo seletivo da [incorporadora], você entende que a [incorporadora] irá tratar seus dados pessoais para a finalidade de avaliar seu currículo e, eventualmente, contatá-lo sobre próximas etapas do processo seletivo. Podemos compartilhar seus dados com empresas que nos auxiliam em processos seletivos e com empresas do grupo da [incorporadora]. Encerrado o processo seletivo, caso não tenha sido selecionado, armazenaremos os seus dados por [12] meses, quando serão descartados, exceto se tivermos alguma obrigação de mantê-lo ou precisarmos desses dados para defendermos nossos direitos. Você pode saber mais sobre como tratamos seus dados pessoais acessando nossa Política de Privacidade ou entrando em contato conosco [inserir canais de contato].

(iii) Caso a incorporadora tenha alguma política de diversidade, informações a respeito de etnia, orientação sexual, saúde e outras podem ser requeridas, mas a resposta deve ser opcional, por serem dados sensíveis. Também nesse caso, sugere-se a inclusão de aviso específico, conforme segue:

A [incorporadora] está comprometida com a igualdade de oportunidades e não desqualifica qualquer candidato em razão de sua origem, gênero, orientação sexual, idade, etnia ou estado civil. Encorajamos a sua candidatura, nos termos da nossa Política de Diversidade, mas você não é obrigado a compartilhar quaisquer dados dessa natureza conosco se não estiver confortável. Caso tenha qualquer dúvida, entre em contato conosco [inserir canais de contato].

(iv) Verificar o nível de adequação de terceiros que auxiliarão no processo seletivo, como consultorias em Recursos Humanos, agências de recrutamento ou integradoras, no caso de estágio;

(v) Verificar se a incorporadora utiliza plataformas de terceiros para o recrutamento (como Gupy, Kenoby, LinkedIn ou outras) e checar se a triagem de currículo se dá por decisão automatizada e, caso positivo, informar os candidatos (ver item 8). Com os perfis interessados em mãos, a incorporadora avalia as pessoas por meio de processos distintos, incluindo triagem de currículos, entrevistas, testes práticos, dinâmicas de grupo ou outras. Nessa etapa algumas empresas realizam checagens de veracidade dos currículos ou histórico criminal.

/ Na prática

Quanto ao processo de seleção, destacamos os seguintes pontos de atenção em relação à proteção de dados:

- (i)** Abster-se de realizar perguntas com fins discriminatórios ou que possam constranger o candidato;
- (ii)** Evitar buscar as redes sociais do candidato com propósito de inferir dados sensíveis, como orientação política ou convicção religiosa. Caso dados sensíveis sejam acessados, não os anotar na ficha do candidato;
- (iii)** Evitar pedir ou buscar antecedentes criminais, exceto se necessário para o exercício da função⁸, quando poderá ser feito e informado ao candidato;
- (iv)** Abster-se de pesquisar o score de crédito do candidato. Caso necessário no caso concreto, informar os candidatos deste requisito.

⁸ Conforme decisão do TST, a empresa pode verificar antecedente criminal quando “amparada em expressa previsão legal ou justificar-se em razão da natureza do ofício ou do grau especial de fidúcia exigido, a exemplo de empregados domésticos, cuidadores de menores, idosos e pessoas com deficiência, em creches, asilos ou instituições afins, motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, bancários e afins, trabalhadores que atuam com substâncias tóxicas e entorpecentes e armas, trabalhadores que atuam com informações sigilosas”. (IRR-243000-58.2013.5.13.0023)

2.2. Admissão

No momento da admissão, a incorporadora irá apresentar o contrato de trabalho ao futuro empregado e coletar alguns documentos adicionais, como carteira de trabalho, dados de dependentes – a depender da oferta de benefícios –, dados bancários e outros. Nesse cenário, recomenda-se a inclusão de cláusulas específicas no contrato de trabalho, além de incluir um treinamento básico de proteção de dados pessoais como treinamento obrigatório. Via de regra, a incorporadora irá valer-se da base legal de execução de contrato e de cumprimento de obrigação legal para o tratamento de dados nessa fase.

/ Na prática

No momento da admissão, recomenda-se:

- (i)** Incluir cláusula específica de proteção de dados no contrato de trabalho, de forma a dispor a obrigação de observância das políticas internas relacionadas ao tema (ver item 4), as principais finalidade e bases le-

gais para tratamento de dados pessoais de empregados pela incorporadora, a possibilidade de a empresa monitorar sistemas e acessos realizados no ambiente de trabalho e outras;

(ii) Informar todos os terceiros provedores de benefícios que terão acesso aos dados do colaborador, como vale refeição, seguro de vida e de saúde, assistência odontológica e outros, conforme aplicável;

(iii) Certificar-se de que os contratos com esses terceiros contam com cláusulas específicas de proteção de dados; e

(iv) Treinar os colaboradores em relação às políticas internas de proteção de dados, incluindo de segurança da informação e resposta a incidentes.

⁸ Conforme decisão do TST, a empresa pode verificar antecedente criminal quando “amparada em expressa previsão legal ou justificar-se em razão da natureza do ofício ou do grau especial de fidúcia exigido, a exemplo de empregados domésticos, cuidadores de menores, idosos e pessoas com deficiência, em creches, asilos ou instituições afins, motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, bancários e afins, trabalhadores que atuam com substâncias tóxicas e entorpecentes e armas, trabalhadores que atuam com informações sigilosas”. (IRR-243000-58.2013.5.13.0023)

2.3. Monitoramento de empregados

É prerrogativa do empregador o monitoramento e acompanhamento de suas atividades, o que deve ser feito de forma proporcional. Alguns monitoramentos devem ser realizados inclusive para assegurar a proteção de sistemas e de dados pessoais e tais medidas devem ser claras aos colaboradores. Em geral, a base legal utilizada para o monitoramento é o legítimo interesse da incorporadora.

/ Na prática

Quanto ao monitoramento de empregados, recomenda-se:

- (i)** Limitar acessos do empregado a sistemas e conteúdo que a empresa entende não serem apropriados à função ou ao ambiente de trabalho. A limitação de acesso é medida mais efetiva e mais apropriada em comparação com o constante monitoramento para posterior aplicação de penalidades àqueles que foram “pegos” acessando o sistema ou conteúdo; e
- (ii)** Informar ao empregado sobre as formas de monitoramento, como circuito fechado de TV, controle de ponto, acesso ao e-mail e comunicações, entre outras.

2.4. Desligamento e arquivamento

Encerrada a relação de trabalho, por qualquer motivo, a incorporadora deve proceder com o término do contrato, realizando todos os procedimentos necessários para tanto. A partir desse momento, os dados pessoais do ex-colaborador a serem mantidos pela empresa têm novas finalidades: (i) defender-se em possível ação judicial; e (ii) manter histórico da participação do colaborador nas atividades, especialmente atividades que exigem licença para atuar (como engenheiros responsáveis por obras). Para a finalidade descrita no item (i) a empresa pode valer-se da base legal de exercício regular de direitos em processo judicial e, em relação ao (ii), a depender do caso, poderá ser cumprimento de obrigação legal ou atendimento ao legítimo interesse da empresa.

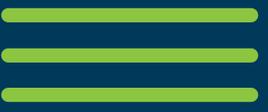
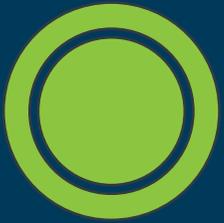
/ Na prática

Quanto ao desligamento de empregados, a incorporadora deve:

- (i) Realizar todas as ações previstas em lei para o desligamento do colaborador, entregando ao titular cópias de documentos a que tem direito;
- (ii) Implementar um procedimento para responder requisições de ex-colaboradores, especialmente relativos a acesso aos dados pessoais e obtenção de cópias de documentos;
- (iii) Arquivar os dados do colaborador pelo tempo necessário, excluindo-os quando encerrada a finalidade.

3

Fornecedores, parceiros e terceiros em geral



É natural que empresas atuem em conjunto com parceiros e fornecedores para melhorar a eficiência de seus serviços. É o caso das imobiliárias parceiras, das administradoras de condomínio e das empreiteiras, por exemplo. Na contratação desses terceiros, é importante que a incorporadora se certifique de que haja um nível mínimo de adequação – o que pode ser feito por meio de um checklist prévio à contratação – e inclua cláusulas específicas a esse respeito nos seus contratos. Tanto o nível de adequação quanto a complexidade das cláusulas deve ser verificada caso a caso, considerando o volume e a criticidade dos dados a que o terceiro terá acesso.

Uma cláusula adequada deve garantir, em geral, que a empresa:

- (i)** tratará os dados apenas para as finalidades do contrato, conforme instruções da incorporadora;
- (ii)** informará a incorporadora imediatamente caso receba solicitações de exercício de direitos de titulares ou tenha ciência de incidentes;
- (iii)** atenderá, conforme instruções da incorporadora os pedidos de direitos de titulares;
- (iv)** adotará medidas de segurança da informação adequadas à criticidade dos dados tratados;
- (v)** permitirá a realização de auditorias, pela incorporadora ou por terceiro por ela indicado, sobre o cumprimento dos requisitos de proteção dos dados pessoais; e
- (vi)** responsabilizar-se-á integralmente por tratamentos ilícitos ou que desrespeitem as instruções da incorporadora.

Do outro lado, a incorporadora também deve considerar que os terceiros e seus empregados são titulares de dados pessoais e todos os princípios e disposições legais se aplicam. Para dar transparência e prestar informação, recomenda-se elaborar uma política de contratação de fornecedores para tratar sobre a forma de tratamento dos seus dados pessoais. Uma política específica para corretores é fortemente recomendada, a qual pode ser disponibilizada em diversos canais de contato, inclusive nas páginas de cadastro da incorporadora, se houver.



3.1. Vendedores de terrenos

A relação com os proprietários de terrenos também deve seguir todos os princípios e requisitos da lei. Destacam-se abaixo alguns cenários e pontos de atenção.

(i) Contato proativo da incorporadora. Caso a incorporadora tenha interesse em um terreno ou imóvel específico, ela pode contatar o proprietário ou o corretor responsável, se houver. Esse contato inicial pode se dar com base no legítimo interesse da incorporadora, demonstrada a expectativa do proprietário. Se o imóvel estiver anunciado para venda, essa expectativa é mais clara. Caso não haja clara comunicação da intenção de venda, a incorporadora pode realizar um contato, mas deve evitar insistir caso não haja resposta ou negativa.

(ii) Contato pelo próprio proprietário. A incorporadora pode ainda disponibilizar um meio de contato (no site, por exemplo) para receber contatos de proprietários que queiram vender seus imóveis. Nesse caso, o formulário de contato deve seguir as mesmas práticas apontadas no item **1.1.**

(iii) Negociação. Nessa fase, destaca-se a necessidade de adotar mecanismos de transparência com esses titulares em relação à realização de due diligence e outras atividades de tratamento de dados pessoais nem sempre percebidas pelos proprietários.

Em termos gerais, especialmente se houver compartilhamento dos dados com terceiros, recomenda-se incluir cláusula contratual no compromisso de compra e venda indicando que:

O Vendedor recebeu e está ciente da Política de Privacidade da [incorporadora]. O Vendedor compreende que, para a regular execução deste Contrato, a [incorporadora] tratará dados pessoais do Vendedor, tais como dados de identificação (como nome completo, estado civil, profissão, RG, CPF) e dados de pagamento. Os dados são necessários para a execução do objeto do Contrato ou para atender a interesses legítimos da [incorporadora], sempre que estes não se sobrepujerem aos direitos do Vendedor.

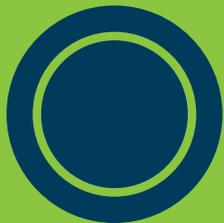
§ 1º *A [incorporadora] se compromete a tratar os Dados Pessoais do Vendedor de acordo com a política de privacidade disponibilizada. Ainda, quando houver necessidade, a [incorporadora] poderá compartilhar os dados pessoais com seus fornecedores, parceiros, órgãos da Administração Pública ou terceiros autorizados para que a [incorporadora] ou tais terceiros possam resguardar seus direitos em relação às obrigações aplicáveis.*

§ 2º *Caso o Vendedor tenha qualquer dúvida em relação ao tratamento de seus Dados Pessoais pela [incorporadora] ou queira requerer o exercício de qualquer direito, este poderá utilizar os canais disponíveis para tanto, nos termos da Política de Privacidade.*

4

Governança de privacidade

As incorporadoras, por relacionarem-se com diversos parceiros, fornecedores e colaboradores, apresentam estrutura complexa de tratamento de dados pessoais. A criação e implementação de um programa de governança em privacidade e proteção de dados revela-se medida adequada para garantir a internalização da LGPD no dia a dia de atividades, estabelecendo as melhores práticas para o tratamento de dados pessoais de acordo com o volume de operações, a escala e a estrutura da incorporadora, assim como o risco de danos aos titulares.



4.1. Boas práticas de organização e funcionamento

O objetivo de estruturar um programa de governança em privacidade e proteção de dados é definir padrões para as atividades da incorporadora que dependam do uso de dados pessoais, documentá-las e tornar possível a verificação periódica dessas práticas.

/ Na prática

De forma geral, o programa deve:

- (i)** demonstrar o comprometimento na adoção de processos e políticas internas que assegurem o cumprimento da regulação e boas práticas relativas à proteção de dados pessoais;
- (ii)** ser aplicável a todo o conjunto de dados pessoais que estejam sob controle da incorporadora, independentemente do modo de coleta;
- (iii)** adequar-se à estrutura, à escala e ao volume das operações;
- (iv)** estabelecer políticas e salvaguardas adequadas com base em processos de avaliação sistemática de impactos e riscos à privacidade;

(v) visar ao estabelecimento de uma relação de confiança com os titulares de dados pessoais, por meio de atuação transparente e que assegure mecanismos de participação;

(vi) estar integrado à estrutura geral de governança da incorporadora, estabelecendo e aplicando mecanismos de supervisão internos e externos;

(vii) contar com planos de resposta a incidentes e procedimentos de remediação; e

(viii) ser atualizado constantemente com base em informações obtidas por meio de monitoramento contínuo, avaliações periódicas e novos preceitos regulatórios.

4.2. Políticas

A consolidação de um programa de governança em privacidade e proteção de dados passa, necessariamente, pelo desenvolvimento e implementação de políticas internas e externas, incluindo a atualização das já existentes. O sucesso do programa dependerá de **(i)** revisão periódica do programa de governança, com definição de metodologia de revisão, equipe responsável e mecanismos para comunicação interna do resultado; e **(ii)** treinamentos e conscientização, com definição de periodicidade, formatos, público alvo e conteúdo abordado.

/ Na prática

Devem ser elaborados documentos e políticas relacionados a:

(i) Política de Privacidade e Proteção de Dados Pessoais, identificando e detalhando as atividades de tratamento realizadas pela incorporadora;

(ii) Política de Segurança da informação, continuidade dos negócios e Manual de Resposta a Incidentes, de viés mais técnico, estabelecendo os padrões e regras de segurança adotados pela incorporadora e as ações a serem tomadas no caso da ocorrência de incidentes;

(iii) Política de Exercício de Direitos dos Titulares, estabelecendo os canais de comunicação, equipes responsáveis, fluxos internos e procedimentos para registro e atendimento de pedidos;

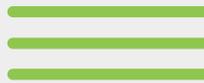
(iv) Política de Relação com fornecedores e parceiros, com lista de requisitos e regras para aprovação, contratação e registro;

(v) Política de Privacidade Interna (recursos humanos), com informações relacionadas ao tratamento de dados de colaboradores, além de uma política específica para corretores associados, se houver;

(vi) Política de Retenção e definição do ciclo de vida dos dados, com regras para armazenamento, acesso, retenção e descarte de dados pessoais tratados;

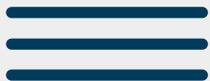
(vii) Política de Cookies e tecnologias similares, especialmente para sites e aplicativos, definindo as tecnologias e regras de utilização; e

(viii) Modelo de Relatório de Impacto à Proteção de Dados Pessoais, com definição das situações que requerem sua elaboração, metodologia a ser aplicada e regras para armazenamento e consulta.



4.3. Ações educativas e mecanismos internos de supervisão

No contexto do desenvolvimento do programa de governança em privacidade e proteção de dados, a incorporadora deve elaborar e implementar ações educativas e de conscientização de seus colaboradores.



/ Na prática

Tais ações devem transmitir a mensagem e os parâmetros ideais de privacidade para toda a empresa, podendo ser organizadas com métodos formais e informais, tais como:

- (i) Métodos formais: treinamentos em sala de aula, aprendizagem online por vídeos e sites, workshops etc.
- (ii) Métodos informais: campanhas visuais no escritório, criação de grupos de discussão sobre temas e acontecimentos do mundo da privacidade e proteção de dados, informes constantes e ativos etc.

/ Exemplos:

/ Antes do lançamento de um empreendimento, os corretores parceiros podem receber treinamento online sobre proteção de dados, abordando em detalhes o programa de governança em privacidade e proteção de dados específico da incorporadora. Isso contribuirá para que o atendimento a clientes seja realizado em sincronia com os as regras e valores da incorporadora.

/ Associações representativas do setor podem criar grupos de discussões sobre privacidade e proteção de dados, abordando temas cotidianos das incorporadoras, visando conscientização e unidade de entendimentos e condutas no setor. Em cada encontro um informe pode ser produzido para envio aos associados.



PARTE II

Nesta parte apresentaremos os principais conceitos da lei, indicando exemplos e formas de cumprir as regras de proteção de dados.



5

Conceitos



Alguns conceitos são essenciais para compreender a LGPD e sua aplicação nas atividades das incorporadoras:

5.1. Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável (aquela que pode vir a ser identificada). Estão inseridas no conceito de dado pessoal não apenas aquelas informações que diretamente identificam pessoas – como nome, RG, CPF, endereço e telefone –, mas também aquelas que, agregadas com outras, podem levar à identificação de um indivíduo, como histórico de transações, identificadores eletrônicos (IP, cookies etc.) e perfis comportamentais em geral.

5.2. Dado pessoal sensível: categoria de dado pessoal que, por revelar características da esfera íntima do indivíduo e potencializar situações discriminatórias, requer proteção especial. Essa categoria inclui dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, saúde, vida sexual, dentre outros.

5.3. Dado anonimizado: tipo de dado que não pode ser vinculado ao titular. A anonimização, processo que deve contar com a utilização de meios técnicos razoáveis e disponíveis, impossibilita a reidentificação dos dados pessoais ou a individualização do titular. Em razão disso, os dados anonimizados não são considerados dados pessoais e estão fora do escopo da LGPD.

5.4. Dado pseudonimizado: tipo de dado que, em razão da utilização de boas técnicas organizacionais e de segurança, só pode ser vinculado ao titular pelo próprio agente de tratamento, necessariamente com a utilização de outros dados em sua posse, mantidos em ambiente apartado.

5.5. Tratamento: toda e qualquer operação realizada com dados pessoais, como coleta, recepção, classificação, acesso, reprodução, processamento, arquivamento, armazenamento, eliminação, modificação, transferência etc.

5.6. Titular: pessoa física a quem se referem os dados pessoais.

5.7. Controlador: pessoa natural ou jurídica a quem cabem as decisões relacionadas ao tratamento de dados pessoais.

5.8. Operador: pessoa natural ou jurídica que realiza o tratamento de dados pessoais conforme comandos do controlador.

5.9. Transferência internacional: transferência de dados para país estrangeiro ou organismo internacional do qual o país seja parte.

5.10. Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública federal, dotado de autonomia técnica e decisória, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD. A Autoridade foi concebida como órgão integrante da Presidência da República, mas a própria LGPD prevê a possibilidade de sua transformação em órgão da administração indireta, com regime de autarquia, após dois anos de seu funcionamento.

6

Princípios

A LGPD estabelece dez princípios que devem ser observados em todas as atividades de tratamento de dados pessoais. A adequação de um produto ou processo deve atentar-se ao atendimento a esses dez princípios e identificar uma base legal⁹ que autorize o tratamento do dado pessoal. A análise *privacy by design* de um processo ou produto busca justamente verificar a conformidade em relação aos princípios de proteção de dados pessoais. Apresentaremos estes dez princípios por meio de uma análise *privacy by design*¹⁰ do seguinte caso:

A Incorporadora XYZ montou um estande para seu novo empreendimento, focado no mercado residencial de luxo. Os promotores desse estande irão coletar alguns dados de possíveis interessados com a finalidade de (i) direcionar o atendimento a um corretor de plantão e (ii) enviar comunicações sobre o empreendimento posteriormente.

⁹ Ver item 7.

¹⁰ Este tema será abordado no item 9.3.



Princípio

Descrição

Na prática

Privacy by design

Finalidade

O tratamento de dados pessoais deve atender a propósitos legítimos, específicos, explícitos e informados aos titulares, vedado tratamento posterior incompatível com tais finalidades.

A incorporadora deve verificar **(i)** se o objetivo do tratamento dos dados é lícito, razoável, específico e claro; e **(ii)** como e quando a finalidade do tratamento será informada ao titular.

A Incorporadora XYZ descreve duas finalidades – **(i)** e **(ii)** – e ambas são lícitas, razoáveis, específicas e podem ser informadas ao titular no momento do cadastro.

Adequação

O tratamento de Dados Pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

A incorporadora deve **(i)** adequar os avisos de privacidade e os meios de comunicar as finalidades ao titular e **(ii)** certificar-se de que os meios de tratamento para atingir a finalidade sejam adequados e compatíveis.

A página de cadastro (física ou online) dispõe de maneira clara as finalidades para as quais os dados serão tratados.

A Incorporadora XYZ tinha como prática buscar o perfil do cliente nas redes sociais para entender seu perfil e direcionar o corretor para o atendimento. Ao fazer a análise privacy by design, percebeu que esse tratamento é incompatível com o que se espera da finalidade descrita e decidiu não seguir com esta busca.

Princípio

Descrição

Na prática

Privacy by design

Necessidade

O tratamento deve ser limitado à mínima quantidade de dados pessoais efetivamente necessária para atender às finalidades, restrito aos dados pessoais pertinentes, proporcionais e não excessivos.

A incorporadora deve questionar o motivo de coleta e tratamento de cada dado utilizado para atender a uma finalidade específica. Uma forma prática de realizar essa verificação é listar os dados utilizados e anotar ao lado a finalidade específica de tratamento de cada dado.

A Incorporadora XYZ percebeu que sua ficha de cadastro tinha como campos obrigatórios (i) nome completo, (ii) CPF, (iii) telefone; e (iv) e-mail, sendo que o cliente indicava como queria ser contatado no futuro, podendo selecionar entre telefone ou e-mail. Nesse caso, alterou a ficha para ser obrigatório o preenchimento apenas do campo de contato correspondente à escolha do cliente (e-mail ou telefone).

Livre acesso

A incorporadora deve garantir aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento de dados pessoais, bem como sobre a integralidade de seus dados pessoais.

A incorporadora deve ter meios e canais de contato dedicados para que os titulares possam acessar ou requerer o acesso a seus dados pessoais.

A Incorporadora XYZ indica na ficha de cadastro o canal por meio do qual o cliente pode ter acesso aos seus dados ou obter informações sobre a duração do tratamento, como tempo de guarda do cadastro.

Princípio

Descrição

Na prática

Privacy by design

Qualidade dos dados

A incorporadora deve garantir exatidão, clareza, relevância e atualização dos dados pessoais em seu controle, de acordo com a necessidade e para o cumprimento da finalidade do seu tratamento.

A incorporadora deve certificar-se de que utiliza dados corretos e atualizados, além de disponibilizar ao titular um meio para atualizar ou retificar seus dados pessoais.

A Incorporadora XYZ disponibiliza um canal para o cliente atualizar seus dados, se necessário.

Transparência

Os titulares devem receber informações claras, precisas e facilmente acessíveis sobre os tratamentos de dados pessoais.

A incorporadora deve adotar medidas para informar o titular sobre o tratamento de seus dados pessoais, como **(i)** just-in-time notice¹¹ no caso de cadastros eletrônicos; **(ii)** treinamento dos responsáveis por coletar dados pessoais; **(iii)** disponibilização de um canal de contato para que os titulares possam requerer informações adicionais.

A Incorporadora XYZ incluiu na ficha de cadastro um aviso de privacidade indicando finalidade, meio de tratamento, terceiros com quem os dados serão compartilhados (incluindo a imobiliária), tempo de guarda, canal de contato e link para política de privacidade – ou outro meio de consultá-la.

¹¹ *Just-in-time notices* são breves avisos de privacidade que aparecem conforme o titular avança no preenchimento dos campos. Ex.: vamos compartilhar seu nome com o corretor para atendimento aqui no estande.

Princípio

Descrição

Na prática

Privacy by design

Segurança

A incorporadora deve utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Este princípio está diretamente relacionado às recomendações do item 10. deste Guia. De forma geral, a incorporadora deve mapear os dados tratados e segmentá-los de acordo com sua sensibilidade e criticidade, implementando medidas de segurança adequadas e proporcionais.

A Incorporadora XYZ mapeou todo o percurso do dado do cliente dentro do estande, desde a recepção até a finalização do atendimento, eliminando acessos desnecessários.

A Incorporadora XYZ implementou medidas de segurança, incluindo controle de acesso, dupla autenticação e registro de acessos ao sistema de cadastro.

Prevenção

A incorporadora deve adotar medidas no sentido de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

A incorporadora deve mapear e registrar os principais riscos a que o titular está sujeito em razão do tratamento de dados realizados e indicar as medidas adotadas para prevenir a ocorrência de danos decorrentes da materialização do risco.

Ciente do risco de o cliente ser importunado por terceiros que tiveram o acesso ao cadastro de forma indevida – como outras imobiliárias e fornecedores de móveis – a Incorporadora XYZ adotou medidas de segurança para minimizar esse risco.

Princípio**Descrição****Na prática*****Privacy by design*****Não-discriminação**

A incorporadora não deve tratar dados pessoais para fins discriminatórios, ilícitos ou abusivos.

A incorporadora não deve tratar dados pessoais ou utilizar o resultado de uma atividade de tratamento para discriminar os titulares.

A Incorporadora XYZ decidiu segmentar a base de dados dos clientes em grupos distintos de acordo com seu perfil e interesse, sem considerar critérios discriminatórios.

Responsabilização e prestação de contas

A incorporadora deve demonstrar a adoção de medidas eficazes e que sejam efetivamente capazes de comprovar a observância e o cumprimento das regras de proteção de dados pessoais, bem como a eficácia dessas medidas.

A incorporadora deve implementar um programa de governança em proteção de dados e manter registro das atividades de tratamento de dados pessoais. O programa deve ter procedimentos para documentar as medidas adotadas para identificar e minimizar riscos decorrentes dessa atividade, como relatórios de impacto de proteção de dados pessoais e atas de reuniões do comitê de privacidade, se houver.

A Incorporadora XYZ redigiu uma política de privacidade acessível ao público, na qual relata a finalidade dos dados tratados, a base legal utilizada, os terceiros com quem os dados são compartilhados, as medidas de segurança adotadas e os direitos dos titulares.

7

Bases legais

Os dados pessoais, triviais ou sensíveis, só podem ser tratados com a utilização de pelo menos uma das hipóteses previstas na LGPD – tais hipóteses são popularmente conhecidas como “bases legais”.



7.1.

Bases legais para Dados Pessoais

A LGPD prevê dez bases legais para o tratamento de dados pessoais. Considerando as particularidades do mercado de incorporações, seis¹² delas merecem destaque:

¹² Além das bases legais destacadas, a LGPD prevê outras quatro hipóteses para o tratamento de dados: (i) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; (ii) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) para a proteção da vida ou da incolumidade física do titular ou de terceiro; e (iv) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Base legal

Escopo

Exemplos

Legítimo Interesse

Tratamento de dados pessoais quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais objeto do tratamento.

/ *Due diligence* de terrenos ou empresas, incluindo emissão de certidões e avaliações de risco, de modo a viabilizar novos negócios.

/ Resposta a clientes que tenham contatado a incorporadora por portais de imóveis ou redes sociais.

Consentimento

Tratamento fundamentado na manifestação livre, informada e inequívoca do titular de dados, autorizando o tratamento para finalidades específicas.

/ Autorização para compartilhamento de dados de comprador de imóvel com empresas de decoração ou outros serviços de seu interesse.

/ Atividades de relacionamento com o cliente – como nos estandes e outros pontos físicos de venda, quando o interessado em imóveis realiza cadastro para viabilizar o atendimento por um corretor.

Base legal

Escopo

Exemplos

Execução de contrato e procedimentos preliminares

Tratamento de dados pessoais quando necessários à execução de contrato do qual o titular seja parte, a pedido do próprio titular.

/ Atividades de elaboração dos contratos de compra e venda com clientes, quando diversos dados legais devem ser coletados, analisados e compartilhados com terceiros envolvidos na operacionalização do negócio.

/ Tratamento de dados de colaboradores quando relacionadas diretamente ao desenvolvimento de suas atividades, embasadas no acordo de trabalho celebrado, incluindo criação de e-mail corporativo, liberação de acesso à rede interna, inclusão em benefícios, pagamento de salário etc.

Cumprimento de obrigação legal

Tratamento de dados pessoais necessários ao cumprimento de obrigações legais ou regulatórias às quais o controlador está vinculado.

/ Guarda obrigatória de documentos operacionais (como contratos comerciais), documentos fiscais e tributários (como guias, notas e livros fiscais), documentos trabalhistas e previdenciários (como contratos de trabalho, termos de rescisão e atestados médicos) e documentos societários (como contratos, atas e livros societários) pelo prazo legal correspondente.

Base legal

Escopo

Exemplos

Exercício regular de direitos em processo judicial, administrativo ou arbitral

Tratamento de dados necessário à atuação e defesa em processos judiciais, administrativos e arbitrais. Engloba o tratamento dos dados disponíveis nos próprios processos, além dos dados em poder da incorporadora e que podem ser utilizados no âmbito de processos ativos.

/ Acompanhamento de processos pela incorporadora, com armazenando dos respectivos dados em sistema interno.

/ Transferência de documentos atinentes a processo aos advogados responsáveis.

/ Utilização de documentos em processos.

Proteção do crédito

Possibilita o tratamento de dados pessoais para análise de crédito e verificação de capacidade financeira de clientes.

/ Análise de dados financeiros do cliente – como comprovantes de renda e score de crédito – para tomada de decisão quanto a modalidades de financiamento do imóvel.

/ Coleta de dados junto a birôs de crédito para avaliação do risco de inadimplência e aplicação de taxa de juros.

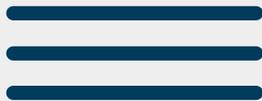
Considerando suas particularidades e relevância na rotina das incorporadoras, abordaremos em maior detalhe as bases legais do legítimo interesse e do consentimento.

7.1.1. Legítimo interesse

O legítimo interesse é uma base legal aberta que permite a controladores e operadores tratarem dados pessoais para situações concretas que não sejam proibidas por lei e que não conflitem com direitos e liberdade individuais dos titulares. Para ser válido, esse tratamento deve ter como referências uma finalidade legítima, uma expectativa aceitável do titular e deve ocorrer somente com o uso de dados necessários, dando transparência ao titular e observando também seus direitos, previstos na LGPD.

Os interesses legítimos almejados devem ser do próprio agente de tratamento ou de terceiro, sendo que a própria LGPD exemplifica as situações de apoio e promoção das atividades do controlador e de prestação de serviços que beneficiem o titular de dados pessoais como exemplos de aplicação do legítimo interesse.

Por ser uma base aberta, o legítimo interesse concede considerável liberdade e autonomia para controladores utilizarem-na em novos modelos de negócio ou situações em que o consentimento simplesmente não é possível do ponto de vista prático.



/ Na prática

Para justificar o tratamento com base no legítimo interesse é necessário que algumas premissas sejam atendidas pelo controlador – tais premissas podem ser organizadas em Condições Essenciais e Condições de Validade:

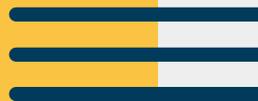
Condições Essenciais

/ Necessário verificar se a atividade de tratamento a ser realizada envolve direitos e liberdades fundamentais do titular e se esses direitos prevalecem em relação aos interesses do controlador.

/ O uso do legítimo interesse sempre deve ser feito com fundamento em uma situação concreta.

X

Caso prevaleçam direitos e liberdades fundamentais do titular ou se não for identificada uma situação concreta que revele a necessidade de tratamento de dados, a base legal do legítimo interesse não poderá ser utilizada.



Condições de Validade

/ O tratamento deve ser realizado para finalidades legítimas do controlador.

/ O titular de dados deve ter uma legítima expectativa sobre o tratamento - deve existir efetivo balanceamento entre as finalidades do tratamento e as expectativas do titular, sobretudo em vista dos seus direitos e liberdades fundamentais.

/ Apenas dados estritamente necessários ao cumprimento das finalidades devem ser tratados.

/ As práticas devem ser transparentes, fornecendo informações claras e precisas aos titulares sobre o tratamento de seus dados pessoais.

/ Devem ser observados os princípios de proteção de dados.

/ Devem existir salvaguardas para proteger os dados pessoais tratados, assim como medidas dedicadas à mitigação de riscos (por exemplo, segregação lógica de bases de dados, implementação de controles de acesso às bases de dados e o uso de técnicas de anonimização e pseudonimização).

! A LGPD estabelece que a ANPD poderá solicitar, a qualquer tempo, a justificativa documentada da adequação de qualquer tratamento baseado no legítimo interesse.



7.1.2. Consentimento

Para utilizar o consentimento - manifestação livre, informada e inequívoca do titular de dados, autorizando o tratamento para finalidades específicas - o controlador deverá se atentar para o atendimento dos seguintes requisitos:

Livre:

a manifestação do titular deve ser uma ação espontânea, que não seja objeto de pressão ou ameaça de nenhuma natureza. O titular deve ter a opção de não dar o seu consentimento para a finalidade específica almejada pelo controlador, sem que isso acarrete consequências negativas além daquelas das quais a ausência de consentimento derive diretamente.

/ Na prática

- (i) A não utilização dos dados pessoais do titular para a finalidade determinada deve ser a única consequência de eventual recusa do consentimento pelo titular;
- (ii) O titular deve receber informações sobre a possibilidade de não fornecer seu consentimento, incluindo explicação sobre as eventuais consequências de tal recusa, e ter a possibilidade de revogar o consentimento já fornecido; e
- (iii) Situações de assimetria de poder entre o controlador e o titular, como no caso da manutenção das relações existentes entre a incorporadora e seus colaboradores - relação trabalhista e/ou de prestação de serviço - requerem maior atenção. Isso porque pode ser argumentado que na maioria das situações não existiria possibilidade de recusa sem potenciais consequências negativas aos colaboradores, o que faria com que eventual consentimento solicitado não fosse considerado livre. No entanto, em casos excepcionais, havendo efetiva possibilidade de recusa por parte do colaborador e sem possibilidade de existirem consequências negativas a este (como nos casos de autorização de uso de imagem de colaboradores para a elaboração de materiais institucionais), o consentimento pode vir a ser considerado livre.

Informado:

o titular deve, no momento do fornecimento do consentimento, ter acesso a todas as informações relevantes sobre o tratamento, as quais podem ser fornecidas por meio da Política de Privacidade da incorporadora.

/ Na prática

(i) É recomendável apresentar, no contexto da obtenção do consentimento do titular, informações claras e objetivas a respeito do tratamento do qual o consentimento depende, incluindo, por exemplo, quais dados pessoais serão tratados, com quais terceiros tais dados serão compartilhados e qual será a finalidade do tratamento e compartilhamento de tais dados.

(ii) Ao longo do processo de obtenção do consentimento, uma boa prática são as chamadas just-in-time notices, em que são apresentadas “pílulas de informação” ao titular; da mesma forma, práticas de consentimento granular (diferentes checkboxes ao invés de somente um) são também boas práticas;

(iii) Para manter a transparência mesmo após o consentimento, é importante sempre fornecer fácil acesso para a Política de Privacidade ou outros documentos aplicáveis.

Inequívoco:

o consentimento só será considerado legítimo quando houver demonstração da efetiva manifestação de vontade do titular - isto é, por meio de uma ação afirmativa de sua parte.

/ Na prática

É recomendável que o controlador tenha condições de verificar se o titular realizou alguma ação afirmativa no fornecimento do consentimento, como assinatura em um termo de consentimento em papel ou a seleção voluntária de um checkbox em sistemas eletrônicos (quando o titular estiver devidamente identificado/autenticado). A ideia de “concordância tácita” com termos de uso, regimentos internos ou com uma política de privacidade disponibilizada pela incorporadora e não necessariamente validada pelos titulares não poderá ser considerada uma ação afirmativa de fornecimento de consentimento.

Sempre que o tratamento for baseado no consentimento, o controlador deverá dispor de mecanismos que possibilitem a gestão, pelo titular, do consentimento fornecido (inclusive por meio de consulta sobre o escopo do consentimento e pela possibilidade de exercício do seu direito de revogar o consentimento); e que registrem a forma e o momento de obtenção do consentimento. É possível realizar tais tarefas de forma automatizada, utilizando ferramentas como:

Consent Management Platforms (CMPs)

Ferramentas de software, próprias ou de terceiros, que permitem a gestão do consentimento do titular em meios digitais, criando uma espécie de “histórico digital” das interações do usuário com a aplicação.

Privacy Dashboards

São áreas do site ou aplicativo do controlador, que permitem o exercício dos direitos dos titulares de forma facilitada e intuitiva, por meio de uma CMP e/ou outras soluções de software conectadas a essa página.

7.2.

Bases legais para Dados Sensíveis

Quando o tratamento envolver dados sensíveis, a LGPD privilegia o uso da base legal do consentimento, devendo as demais bases ser aplicadas apenas na impossibilidade de obtenção de consentimento e exclusivamente quando o tratamento for imprescindível para o atingimento das finalidades pretendidas.

Considerando as atividades das incorporadoras, merece destaque, além do consentimento, a base legal de garantia da prevenção à fraude e à segurança do titular, também aplicável ao tratamento de dados pessoais sensíveis¹³:

¹³ A LGPD prevê, para além do consentimento e da garantia da prevenção à fraude e à segurança do titular, a possibilidade de tratamento de dados sensíveis nas seguintes hipóteses: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (iii) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; (iv) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; (v) proteção da vida ou da incolumidade física do titular ou de terceiro; e (vi) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Base legal

Escopo

Exemplos

Consentimento

Para dados sensíveis, além dos requisitos mencionados no item 4.1.2., o consentimento também deve ser destacado.

O destaque está relacionado à necessidade de se reservar espaço dedicado (seja no contexto de um termo, autorização, contrato ou até de uma relação verbal) exclusivamente para que o titular possa manifestar, de forma positiva, a sua vontade de autorizar o tratamento de seus dados sensíveis para finalidades informadas.

/ Caso a incorporadora deseje iniciar um programa de incentivo à prática de atividades físicas entre seus colaboradores e, para tanto, necessite coletar e compartilhar dados de saúde com uma consultoria especializada, deverá, no momento da adesão, apresentar ao colaborador as regras do programa e coletar o respectivo consentimento destacado para o tratamento de dados sensíveis.

Garantia da prevenção à fraude e à segurança do titular

Tratamento de dados sensíveis para processos que visam à garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos do titular, e exceto no caso de prevalecerem direitos e liberdades fundamentais que exijam a proteção dos dados.

/ Coleta de dados biométricos de colaborador para acesso a sistemas financeiros da incorporadora.

7.2.1. Garantia da prevenção à fraude e à segurança do titular

Há uma discussão sobre a possibilidade de utilização da base legal de garantia da prevenção à fraude e à segurança do titular para fins de utilização de dados biométricos para controle de ponto ou acesso ao estabelecimento. Nesses casos, a incorporadora deve avaliar se os quatro requisitos da base legal foram atendidos, além de observar todos os princípios.

¹⁴ Vide item 5.

¹⁵ Artigo 10, II, LGPD

/ Na prática

(i) Finalidade de garantia da prevenção à fraude e à segurança do titular: o objetivo primordial do processo deve ser a segurança do próprio titular, não do controlador. Portanto, caso a finalidade maior seja garantir a segurança das instalações e dos ativos da empresa, é preciso rever a aplicabilidade da base legal.

(ii) Utilização do dado em processos de identificação e autenticação de cadastro em sistemas eletrônico: o dado sensível só pode ser utilizado para reconhecer o titular ou certificar a veracidade de cadastro em sistema eletrônico.

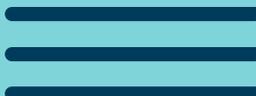
(iii) Obrigação de resguardar os direitos mencionados no art. 9º da LGPD¹⁴: reforço da obrigação de que o controlador deve fornecer informações acerca da finalidade, forma e duração de tratamento, identificação do controlador e suas informações de contato, hipóteses de uso compartilhado, responsabilidade dos agentes e direitos do titular. Note-se que o reforço não significa repetição: pelo princípio de que “a lei não possui palavras inúteis”, significa que esse é um tema que precisa de cuidado redobrado pelo controlador, inclusive aplicando-se interpretações mais restritivas.

(iv) Não podem prevalecer direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais: da mesma forma que na utilização da base legal do legítimo interesse¹⁵, caso os direitos e liberdades fundamentais do titular previstas na constituição devam prevalecer, esta base legal não pode ser utilizada.

8

Direitos dos titulares

A LGPD trouxe uma série de direitos que os titulares podem requerer aos controladores dos dados pessoais. Alguns desses direitos decorrem do cumprimento dos princípios – já analisados no item 0 deste Guia – e outros da correta aplicação das bases legais, conforme avaliado no item 0. Neste tópico, vamos analisar os direitos previstos no Capítulo III da LGPD, denominado “dos direitos do titular”. O objetivo é analisar cada um desses direitos, indicando seu escopo e possíveis limitações.



Direito	Escopo	Aplicabilidade e limitações	LGPD	Prazo
Confirmação de existência de tratamento	Obter do controlador uma declaração de que seus dados são tratados pela incorporadora.	Aplicável ao tratamento baseado em qualquer base legal.	art. 18, I	Declaração simplificada: imediata Declaração completa: 15 dias
Acesso	Obter do controlador acesso aos seus dados tratados pela incorporadora.	Aplicável ao tratamento baseado em qualquer base legal. Poderá haver limitações baseadas na proteção do segredo comercial e industrial, conforme o caso.	art. 18, II	Declaração simplificada: imediata Declaração completa: 15 dias
Recebimento de cópia integral	Receber cópia integral dos dados tratados pela incorporadora.	Aplicável quando a base legal for consentimento ou execução de contrato. Poderá haver limitações baseadas na proteção do segredo comercial e industrial, conforme o caso.	art. 19, § 3º	Não há previsão legal

Direito	Escopo	Aplicabilidade e limitações	LGPD	Prazo
Correção	Corrigir os dados incompletos, inexatos ou desatualizados sob controle da incorporadora, a pedido do titular.	Aplicável ao tratamento baseado em qualquer base legal. A incorporadora deve certificar-se de que o titular apresenta informação correta com seu pedido de correção.	art. 18, III	Não há previsão legal
Anonimização, bloqueio ou eliminação	Anonimizar (passar o dado por um processo que não permita mais à incorporadora a identificação do titular); bloquear (tornar o dado inacessível) ou eliminar (excluir o dado da base).	Aplicável quando os dados forem desnecessários, excessivos ou tratados em desconformidade, como quando não há mais uma base legal válida (ex.: opt-out em lista de e-mail marketing criada com base no legítimo interesse).	art. 18, IV	Declaração simplificada: imediata Declaração completa: 15 dias

Direito	Escopo	Aplicabilidade e limitações	LGPD	Prazo
Portabilidade	Possibilidade de mudar de fornecedor de produto ou serviço para outro, levando consigo uma cópia de seus dados pessoais em formato interoperável.	<p>Aplicável, a princípio, a todos os casos, pendente de regulamentação futura da ANPD.</p> <p>Poderá haver limitações baseadas na proteção do segredo comercial e industrial, conforme o caso.</p>	art. 18, V	Não há previsão legal
Eliminação	Excluir do dado, a pedido do titular, caso seja requerido pelo titular e quando não houver outro motivo legítimo para manter o dado.	<p>Aplicável quando a base legal for consentimento.</p> <p>A incorporadora deve certificar-se de que o titular apresenta informação correta com seu pedido de correção.</p>	art. 18, VI	Não há previsão legal

Direito	Escopo	Aplicabilidade e limitações	LGPD	Prazo
<p>Informação sobre uso compartilhado</p>	<p>Obter do controlador uma lista das entidades públicas e privadas com as quais o controlador compartilhou os dados.</p>	<p>Aplicável ao tratamento baseado em qualquer base legal.</p>	<p>art. 18, VII</p>	<p>Não há previsão legal</p>
<p>Informação sobre possibilidade de não fornecer consentimento e sobre as consequências da negativa</p>	<p>Informar o titular, no momento da solicitação do consentimento, as consequências de não consentir. (Ex.: você é livre para escolher fornecer seus dados para nós. Porém, caso não consinta, não poderemos fornecer alguns serviços.)</p>	<p>Aplicável quando a base legal for consentimento.</p>	<p>art. 18, VIII</p>	<p>Não há previsão legal</p>

Direito	Escopo	Aplicabilidade e limitações	LGPD	Prazo
Revogação do consentimento	Informar o controlador sobre o término do consentimento, deixando claro que a partir dali não haverá autorização para tratamento de dados realizado com esta base legal.	Aplicável quando a base legal for consentimento. Não prejudica o tratamento de dados anterior e não pressupõe a exclusão dos dados tratados anteriormente	art. 18, IX	Não há previsão legal
Oposição	Informar o controlador que não concorda com o tratamento de dados pessoais realizado (Ex.: após recebimento de um e-mail marketing, decide opor-se e sai da lista - unsubscribe. A partir desse momento, a incorporadora não tem legítimo interesse para enviar e-mail marketing a esse titular.)	Aplicável a todos os casos, exceto quando a base legal for consentimento. Neste caso, poderá valer-se da revogação do consentimento.	art. 18, § 2º	Não há previsão legal

Direito	Escopo	Aplicabilidade e limitações	LGPD	Prazo
Revisão	<p>Informar o titular sobre a existência de um processo de decisão automatizada e, caso requerido pelo titular, submeter essa decisão a um processo de revisão.</p> <p>(Ex.: incorporadora utiliza um software para análise de crédito, o qual define linhas de crédito possíveis com base no perfil do cliente. Incorporadora deve informar o cliente e permitir a revisão da decisão apresentada pelo software.)</p>	Aplicável a casos em que o titular é submetido a uma decisão automatizada.	art. 20	Não há previsão legal

8.1. Exercício de direitos por titulares

Conforme previsto na LGPD, o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador e perante a autoridade nacional. As incorporadoras devem estar prontas para receber um volume considerável de requisições, especialmente no início da vigência da legislação, atenta aos prazos de resposta.

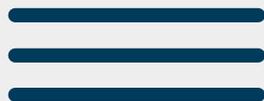
Além disso, deve ser definido internamente um procedimento de checagem da identidade do titular. O procedimento de verificação de identidade de um titular que requer acesso aos dados é bastante relevante visto que, caso a incorporadora acabe fornecendo dados para pessoas não autorizadas, pode ser caracterizado um incidente.

Nesse sentido, seguindo as melhores práticas, deve-se verificar a identidade do titular por meio de procedimento que **(i)** não colete ainda mais dados de forma desproporcional ao pedido feito e **(ii)** dificulte o acesso do titular aos seus direitos garantidos por lei.

Não há um modelo único e ideal para checagem de identidade e cada incorporadora deve verificar os dados que coleta de cada categoria de titular e o que seria razoável. Algumas opções são **(i)** pedir ao requerente para confirmar dados que a empresa tenha em seu banco para identificar o titular ou **(ii)** verificar documentos oficiais do requerente para checar sua identidade. Qualquer procedimento adotado deve ser documentado e refletido no treinamento daqueles que trabalham diretamente com o público externo.

8.1.1. Atendimento a petições e reclamações de titulares

Considerando os direitos previstos na LGPD e também o artigo 43 do Código de Defesa do Consumidor, que dispõe sobre o dever de disponibilização de informações aos titulares de dados, é essencial que as incorporadoras, enquanto agentes de tratamento de dados pessoais, criem mecanismos para o recebimento e atendimento de solicitações de titulares.



/ Na prática

As seguintes soluções representam boas alternativas:

- (i) Disponibilizar um canal de contato (e-mail, por exemplo) para que o titular possa enviar seus requerimentos de direitos;
- (ii) Desenvolver um privacy dashboard, em atendimento aos requisitos de acessibilidade e transparência, permitindo aos titulares ter acesso a seus dados pessoais e exercer seus direitos diretamente na ferramenta. Para clientes, a incorporadora pode criar uma funcionalidade no portal do cliente para isso; e
- (iii) realizar ajustes nas plataformas e sistemas da incorporadora para que os titulares possam ter acesso a informações sobre o tratamento de seus dados pessoais e, quando cabível, solicitar a exclusão.

É importante mencionar que, quando houver uma solicitação de exclusão de dados por um titular e esta for cabível, toda a cadeia de tratamento de dados também deve providenciar a exclusão - ou seja, a incorporadora terá também que providenciar o encaminhamento da comunicação aos seus parceiros que eventualmente tenham recebido dados do titular solicitante.

Especificamente sobre a criação de canal de contato para requerimento de titulares (item “i” ao lado), é recomendável que, considerando as diversas categorias de titulares com as quais as incorporadoras mantêm relações – colaboradores, clientes, fornecedores etc. – seja realizada a segmentação dos canais de contato, de modo a facilitar o tratamento interno das requisições.

9

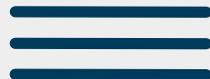
Obrigações impostas aos agentes de tratamento

A LGPD estabelece uma série de obrigações que devem ser seguidas pelos agentes de tratamento – controladores ou operadores. Dentre estas, destacam-se:



9.1. Registro das Atividades de Tratamento

Os controladores e operadores têm a obrigação de manter registro das operações de tratamento de dados pessoais que realizarem. Tal obrigação demanda não só o mapeamento das atividades de tratamento, mas também sua constante revisão e atualização.



/ Na prática

O mapeamento das atividades pode ser realizado com soluções tecnológicas (sistemas que identificam e desenham o caminho dos dados dentro da empresa) ou através de entrevistas e preenchimento de questionários junto às áreas estratégicas da empresa.

Todo o material reunido e classificado constituirá o registro de atividades de tratamento da empresa, que precisará ser constantemente revisto – para tanto pode-se concentrar as tarefas no Encarregado (ou equivalente) ou, de forma descentralizada, atribuir responsabilidade para que as áreas de negócio da empresa estabeleçam processos de revisão periódica do mapeamento das atividades de tratamento.

Exemplos:

/ Após a conclusão do mapeamento das atividades de tratamento da incorporadora, as informações poderão ser armazenadas em ambiente virtual acessível pelos líderes das áreas de negócio – vendas, comercial, marketing, relacionamento com o cliente etc. Sempre que uma nova atividade de tratamento for iniciada o respectivo líder será responsável por efetuar o registro na plataforma criada. O prazo para registro e a responsabilidade por tal ação devem estar previstos em política interna da incorporadora.

/ O registro deve refletir a realidade atual de tratamento de dados pela incorporadora, de modo que é importante estabelecer periodicidade adequada ao modelo de negócio da incorporadora. A ANPD poderá, futuramente, estabelecer prazo de guarda dos registros.

9.2.

Padrões de segurança

A LGPD demanda dos agentes de tratamento a adoção de medidas de segurança, técnicas e administrativas para proteger os dados pessoais – isso inclui impedir acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração e comunicação ou qualquer forma de tratamento inadequado.

Os próprios sistemas utilizados pelos agentes de tratamento devem, também, ser estruturados de forma a atender os requisitos de segurança e boas práticas impostas pela LGPD. Para entender melhor, consultar o item 10 deste guia.

/ Na prática

Surgem como boas práticas de segurança a serem adotadas pelas incorporadoras:

(i) a implementação de hierarquias de acesso aos sistemas e banco de dados;

(ii) a implementação de sistema de identificação eletrônica e autenticação de usuários, de modo a evitar acessos não autorizados;

(iii) o registro e a documentação de todas as etapas de processamento dos dados dentro dos sistemas e realização de verificações internas regulares para garantir que todos os acessos tenham a correta autorização;

(v) o inventário dos registros de acesso às bases de dados da empresa, contendo o momento, a duração, a identificação do colaborador ou do responsável pelo acesso designado e o arquivo acessado;

(vi) sempre que possível, utilização de técnicas de anonimização e pseudonimização para garantir maior segurança dos dados pessoais, especialmente quando se tratar de dados sensíveis, já que possuem maior potencial de dano ao titular; e

(vii) auditoria regular interna e externa em proteção de dados pessoais.

9.3.

Privacy by Design

O conceito de Privacy by Design, também conhecido como “privacidade por concepção”, determina que os agentes de tratamento adotem medidas para proteger os dados pessoais desde a concepção de produtos ou serviços e durante todo os respectivos ciclos de vida.

/ Na prática

Privacidade por design é uma abordagem de engenharia de sistemas desenvolvida nos anos 1990 e que, através de alguns princípios, aponta a necessidade de levar em consideração a privacidade dos usuários durante todo o processo de desenvolvimento de um novo produto ou serviço. É um conceito amplo, que leva em consideração direitos dos titulares, como a autodeterminação informativa, a inviolabilidade da intimidade e direitos humanos. Ainda que haja críticas por essa abordagem ser considerada vaga e de difícil aplicação prática, a LGPD prevê o tema no art. 46, § 2º.

Desmistificando: no contexto jurídico, privacy by design não é nada mais do que cumprir a lei. Ainda que pareça um pleonasma, é importante destacar a função de reforço da LGPD, o que inspira cuidados para as empresas no desenvolvimento de novos software, produtos e serviços. Logo, cada novo projeto, deve ser avaliado em uma perspectiva jurídica, para que as áreas responsáveis pelo desenvolvimento do Projeto possam adequar procedimentos, atividades e códigos para funcionar de acordo com essas orientações, que podem incluir, por exemplo:

- (i) Avaliar a finalidade da coleta dos dados;
- (ii) Quais dados são necessários para o projeto;
- (iii) Quais dados são compartilhados com terceiros e quem são esses terceiros;
- (iv) Quais dados são excessivos e, assim, não devem ser inicialmente coletados;
- (v) Se o projeto traz transparência e explicações claras para o titular, com linguagem de fácil compreensão;
- (vi) A forma como o exercício de direitos pelos titulares será exercida.

9.4. Transferências internacionais

A LGPD determina que a transferência internacional de dados só pode ser realizada caso determinadas hipóteses legais e requisitos de validade sejam atendidos. Contudo, grande parte dos mecanismos previstos depende da atuação da Autoridade Nacional de Proteção de Dados (“ANPD”).

Diante deste cenário, as hipóteses para transferência internacional podem ser esquematizadas da seguinte forma:

Hipóteses de transferência

Para países ou organismos internacionais que proporcionem grau de proteção adequado ao previsto na LGPD

Cláusulas contratuais específicas para determinada transferência

Cláusulas-padrão contratuais

Atuação da ANPD

Avaliação de adequação do país.

Avaliação e definição do conteúdo da cláusula.

Definição do conteúdo da cláusula.

Na prática

Espera-se que a partir da decisão de adequação da ANPD, o fluxo internacional de dados pessoais será viabilizado com este país, sem a necessidade de adoção de salvaguardas adicionais ou qualquer outro tipo de autorização específica por parte da ANPD.

Empresas poderiam elaborar instrumentos contratuais específicos para determinada transferência internacional e submetê-los à aprovação da ANPD.

As cláusulas-padrão contratuais seriam modelos oficiais de instrumentos contratuais, elaborados pela ANPD. Ao adotar tais modelos as empresas não precisariam obter prévia aprovação em seus instrumentos.

Hipóteses de transferência

Normas corporativas globais

Atuação da ANPD

Avaliação e definição do conteúdo das normas.

Na prática

Imagina-se que as normas corporativas globais, quando aprovadas pela ANPD, permitirão o livre fluxo de dados pessoais por empresas do mesmo grupo econômico, ainda que sediadas em países distintos.

Selos, certificados e códigos de conduta regularmente emitidos

Avaliação e definição do conteúdo dos selos, certificados e códigos de conduta.

A obtenção de selos ou certificados ou a adoção de códigos de conduta previamente chancelados pela ANPD viabilizaria o fluxo internacional, sem necessidade de outras aprovações.

Consentimento específico e destacado do titular dos dados pessoais para a transferência

Sem atuação específica.

Titular de dados deve manifestar de forma específica sua autorização para a transferência internacional.

Hipóteses de transferência

Transferência necessária para cumprimento de obrigação legal ou regulatória pelo controlador

Transferência necessária para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados

Transferência necessária para o exercício regular de direitos em processo judicial, administrativo ou arbitral

Atuação da ANPD

Sem atuação específica.

Sem atuação específica.

Sem atuação específica.

Na prática

Transferência seria possível quando necessária para o cumprimento de uma obrigação legal ou regulatória decorrente da legislação brasileira ou uma obrigação estrangeira homologada de acordo com o direito brasileiro.

Quando a transferência internacional dos dados é necessária para a própria execução do contrato que a empresa tem com os titulares.

Quando a transferência internacional dos dados é necessária para a incorporadora ou suas afiliadas atuarem em processo judicial, administrativo ou arbitral.

Importante notar que o armazenamento de dados pessoais em serviços localizados no exterior configura transferência internacional e, assim, requer a utilização de alguma das hipóteses permissivas. Diante disso, é fundamental que as incorporadoras, enquanto agentes de tratamento de dados, elaborem um efetivo mapa de suas transferências internacionais, com identificação dos tipos de dados, destinatários e finalidades – com isso será possível identificar a hipótese de transferência mais adequada e, conseqüentemente, implementar as adequações necessárias para viabilizar as operações.

Exemplos:

/ Caso a incorporadora opte por armazenar os dados de clientes em sistema cloud localizado no exterior, poderá utilizar o consentimento para fundamentar a transferência. Neste caso, é necessário atualizar a Política de Privacidade com informações detalhadas, direcionadas ao cliente, sobre o caráter internacional da operação.

/ Ao se pautar no consentimento, é também necessário operacionalizar a obtenção de consentimento específico e destacado para a transferência, conforme requisitos da LGPD – em sistemas eletrônicos isso poderá ser feito a partir do aceite em um checkbox específico.

10

Encarregado (DPO)

Em sua primeira versão, a LGPD definia o Encarregado como uma “pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional”. A redação foi posteriormente alterada e o termo “natural” foi excluído, abrindo a possibilidade de indicação de uma pessoa natural ou jurídica para o cargo.

Nesse cenário, algumas estruturas são possíveis, sendo que salientamos duas principais, as quais também podem ser combinadas.

Estruturas

Prós

Contras

Nomeação de Encarregado interno

/ Centralização das funções em uma figura clara e identificável por todos na organização

/ Comprometimento da organização com a privacidade e proteção de dados dos titulares, facilitando a integração do DPO na cultura organizacional.

/ Possível sobrecarga de trabalho, caso não haja um time de privacidade e proteção de dados

/ Internalização das demandas e das responsabilidades na empresa

Contratação de Encarregado externo (DPO as a Service)

/ Contratação de equipe especializada

/ Custos variáveis a depender da demanda

/ Comprometimento da organização com a privacidade e proteção de dados dos titulares

/ Ausência de figura interna para contato com demais áreas e titulares colaboradores.

/ Na prática

O escopo de atividades do Encarregado, nos termos do artigo 41 da LGPD, está relacionado a:

- (i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- (ii) receber comunicações da ANPD e adotar providências;
- (iii) orientar os colaboradores e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- (iv) executar as demais atribuições determinadas pela incorporadora, enquanto controladora de dados, ou estabelecidas em regulações complementares.

As informações relacionadas ao Encarregado devem ser disponibilizadas de forma clara e objetiva nos canais de comunicação da incorporadora (site etc.), a fim de que tanto os titulares como os colaboradores da empresa e a ANPD possam entrar em contato.

11

Segurança da Informação

A segurança é um dos princípios que regem a LGPD, demandando que os agentes de tratamento utilizem medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, ou qualquer outra forma de tratamento inadequado ou ilícito.



11.1.

Normas técnicas e padrões de segurança

A LGPD não traz padrões técnicos de segurança da informação específicos a serem seguidos. Em termos de legislação, atualmente o Brasil conta com o regulamento do Marco Civil da Internet para trazer diretrizes nesse sentido. Porém, é possível que a ANPD regule este tema no futuro¹⁶. Sem prejuízo disso, as medidas de segurança da informação devem levar em conta a criticidade dos dados tratados e considerar que medidas de segurança não sanam o descumprimento da legislação como um todo, apenas reduzem o risco de incidentes.

¹⁶O artigo 40 da LGPD prevê expressamente que “a autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência”.

/ Na prática

Considerando as disposições do Marco Civil da Internet e outras obrigações de leis sobre proteção de dados pessoais, sugerimos implementar:

- (i)** Hierarquias de acesso aos sistemas e banco de dados;
- (ii)** Sistema de identificação eletrônica e autenticação de usuários, de modo a evitar acessos não autorizados;
- (iii)** Registro e a documentação de todas as etapas de processamento dos dados dentro dos sistemas e realização de verificações internas regulares para garantir que todos os acessos tenham a correta autorização;
- (iv)** Inventário dos registros de acesso às bases de dados da empresa, contendo o momento, a duração, a identificação do colaborador ou do responsável pelo acesso designado e o arquivo acessado;
- (v)** Sempre que possível, utilização de técnicas de anonimização e pseudonimização para garantir maior segurança dos dados pessoais, especialmente quando se tratar de dados sensíveis, já que possuem maior potencial de dano ao titular; e
- (vi)** Auditoria regular interna e externa em proteção de dados pessoais.

Exemplos:

padrões de segurança merecem especial atenção em situações como:

- A operacionalização do banco de dados de prospects e clientes, que constitui um ativo das incorporadoras e deve ser armazenado em local protegido e em formato que assegure a integridade, disponibilidade e confidencialidade dos dados. Corretores parceiros devem acessar o banco através de mecanismos de autenticação e visualizar apenas os dados dos clientes que de fato atenderão, minimizando assim a possibilidade de vazamento de dados e o compartilhamento com empresas concorrentes.

11.2. Incidentes

O conceito de incidentes contempla toda e qualquer atividade relacionada ao tratamento de dados pessoais realizada em desacordo com os preceitos da LGPD – o não atendimento, por parte do controlador, de um direito exercido pelo titular de dados pessoais configura, assim, um incidente. Incidentes de segurança, por sua vez, referem-se a eventos que impliquem em falha na proteção de dados pessoais em posse do agente de tratamento, prejudicando assim o cumprimento do princípio da segurança.

O artigo 48 da LGPD determina que os controladores deverão comunicar a ANPD e o titular sobre a ocorrência de incidentes de segurança da informação que possam acarretar risco ou dano relevante aos titulares. Para isso, é fundamental a criação de um plano de resposta a incidentes capaz de (i) avaliar os riscos aos titulares derivados do incidente de segurança da informação; (ii) ativar procedimentos internos para que os incidentes de segurança da informação sejam informados à ANPD e aos titulares, quando necessário; e (iii) indicar os procedimentos internos necessários para a continuidade de negócios.

/ Na prática

Um plano eficaz deve definir de maneira clara as etapas que serão internamente seguidas pelo agente de tratamento, desde a identificação do incidente, passando por sua análise e classificação de criticidade, ações de contenção, eliminação e recuperação, até a final elaboração de respostas e notificações cabíveis. Posteriormente, é fundamental que ocorra o monitoramento da efetividade das ações adotadas (vale também se atentar para possíveis efeitos nas esferas judiciais e administrativas).

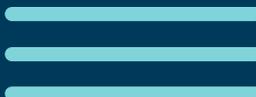
A notificação à ANPD e aos titulares deve mencionar, no mínimo:

- (i) a descrição da natureza dos dados pessoais afetados;
- (ii) as informações sobre os titulares envolvidos;
- (iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- (iv) os riscos relacionados ao incidente;
- (v) os motivos da demora, no caso de a comunicação não ter sido imediata; e
- (vi) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

12

Supervisão, responsabiliza- ção e sanções

A própria LGPD dispõe em seus artigos 52 a 54 as sanções aplicáveis pelo descumprimento da legislação. Porém, as incorporadoras podem sofrer outros tipos de penalidade, como responsabilização no âmbito civil, autuações do Procon, no caso de dados de clientes e investigações do Ministério Público. Neste tópico, avaliaremos a situação atual de cada uma dessas frentes, propondo medidas que podem ser adotadas para reduzir danos.



12.1. ANPD

A ANPD foi criada na LGPD para zelar, implementar e fiscalizar o cumprimento da LGPD em âmbito nacional. As penalidades previstas na LGPD podem variar de uma advertência, com indicação de prazo para adoção de medidas corretivas, até a proibição total do exercício de atividades relacionadas a tratamento de dados – o que pode ser mais danoso que a própria multa de até R\$ 50.000.000,00.

As sanções previstas na LGPD são aplicáveis pela própria ANPD, previsto um regime de dosimetria da pena, o qual levará em consideração¹⁷ diversos fatores, incluindo (i) a boa-fé do infrator; (ii) a cooperação do infrator; (iii) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; e (iv) a adoção de política de boas práticas e governança.

Como pode se observar, esses cinco critérios estão diretamente relacionados à efetividade do programa de governança da incorporadora. A exemplo do que já ocorre em outras regulações¹⁸, a LGPD privilegia o esforço da empresa em adequar-se ao aplicar as penalidades.

/ Na prática

Ao identificar um incidente ou ter alguma inadequação apontada pela ANPD, sugere-se adotar medidas de cooperação com a ANPD, além de demonstrar a efetividade do programa de governança em proteção de dados. Com isso, é possível obter a redução da pena, nos termos da lei.

¹⁷Artigo 52, § 1º, LGPD

¹⁸Exemplificativamente, a lei anticorrupção e seu regulamento, nos termos do artigo 5º, § 4º, Decreto 8.420/2015.

12.2. Procon, Senacon e Ministério Público

Nos temas que são de sua competência, outras autoridades podem vir a atuar como fiscalizadores das regras de proteção de dados, independentemente da efetiva constituição da ANPD – inclusive porque, como visto, não apenas a LGPD dispõe sobre proteção de dados pessoais no Brasil¹⁹. Essas entidades podem investigar e aplicar penalidades, conforme o caso, considerando eventuais práticas inadequadas ou incidentes envolvendo dados pessoais.

Atualmente, tem-se visto uma atuação forte do Ministério Público e da Secretaria Nacional do Consumidor (Senacon), tendo aplicado multas e investigado empresas com práticas mais agressivas de tratamento de dados pessoais. Da mesma forma como foi expressamente previsto na LGPD, as penas, em geral, são mais tênues quando as empresas colaboram com as investigações e prestam informações corretamente.

¹⁹Destaca-se no cenário normativo o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei do Cadastro Positivo

12.3. Contencioso em proteção de dados

Por fim, o próprio titular dos dados pessoais pode pleitear direitos perante as empresas e judicializar demandas de proteção de dados. Da mesma forma que ocorre em outros setores regulados da economia²⁰, o titular pode apresentar reclamações diretamente à empresa, perante a ANPD ou ao judiciário, visando a obtenção de indenizações. Para reduzir danos, recomenda-se que as incorporadoras, com base nas suas atividades de tratamento de dados e fragilidades encontradas, antecipem-se a este cenário e busquem avaliar como mitigar a existência de um contencioso nesse caso.

²⁰Exemplificativamente o setor financeiro, regulado pelo Banco Central, ou de telecomunicações, regulado pela Anatel.

13

Checklist de adequação

Para adequar-se à LGPD e conseguir atender às obrigações legais dispostas na legislação, conforme analisado neste Guia, propõe-se o seguinte passo-a-passo. Estas instruções podem servir como inspiração para que as empresas criem um checklist de medidas que as incorporadoras podem seguir para ter um nível mínimo de adequação.



Ação

- Conscientizar os colaboradores sobre a importância de adequar-se à legislação, por meio de palestras, treinamentos e workshops
- Mapear os processos organizacionais que utilizam dados pessoais
- Avaliar os processos mapeados e identificar os pontos de melhoria e adequação

Objetivo

Familiarizar a organização e seus colaboradores com a metodologia de trabalho e conscientizá-los de que a LGPD deve balizar todo negócio e processo que lide com dados pessoais.

Mapear as atividades de tratamento de dados da organização, as suas relações contratuais com terceiros, os documentos internos relevantes às atividades e qualquer documentação complementar necessária para entender os processos e elaborar o registro de atividades de tratamento²¹.

²¹ Previsto no artigo 37 da LGPD.

Analisar os riscos de violação a preceitos regulatórios e aos direitos dos titulares de cada atividade de tratamento de dados pessoais mapeada, levando em consideração o modelo de negócio, os recursos tecnológicos, a governança e a cultura da organização, com o fim de indicar as medidas de adequação e de diminuição de riscos.

Ação

- Avaliar os contratos com terceiros que tratam dados pessoais para a incorporadora

- Atribuir a base legal a cada um dos processos mapeados

- Atribuir a base legal a cada um dos processos mapeados

- Elaborar relatórios de impacto à proteção de dados pessoais, conforme necessário

- Aditar contratos com terceiros, conforme necessário

Objetivo

Identificar os terceiros que tratam dados pessoais, atribuir nível de criticidade e risco das atividades e verificar se os contratos protegem a incorporadora.

Adequar os processos de tratamento de dados pessoais aos preceitos legais, conforme requisitos de determinadas bases legais e dos princípios aplicáveis.

Obter o registro de atividades de tratamento, contemplando uma visão atualizada e adequada dos processos mapeados, indicando a base legal.

Realizar a análise de risco necessária nos casos de atividades de tratamento de dados de alto risco ou que se valem da base legal do legítimo interesse.

Resguardar-se contratualmente e dispor obrigações específicas de proteção de dados pessoais e segurança da informação.

Ação

- Elaborar políticas específicas de proteção de dados pessoais
- Nomear o Encarregado
- Implementar um canal de contato para receber requisições de direitos de titulares, além de contar com uma ferramenta para tanto
- Revisar as medidas de segurança da informação, reforçando os controles e ferramentas, se necessário
- Treinar colaboradores e corretores, conforme necessário, sobre os novos procedimentos adotados

Objetivo

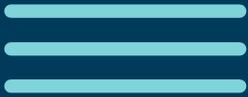
Implementar um programa de governança em privacidade e proteção de dados pessoais.

Designar um responsável pelas práticas de proteção de dados pessoais na incorporadora.

Ter uma ferramenta ou um canal de contato que permita a gestão e resposta das demandas de titulares.

Garantir um nível razoável de proteção aos dados pessoais e evitar incidentes.

Garantir a eficácia das medidas adotadas e alinhar os novos processos com aqueles que estão na linha de frente da operação.



ABRAINC
ASSOCIAÇÃO BRASILEIRA DE
INCORPORADORAS IMOBILIÁRIAS



abrainc.org.br

