POLÍTICA DE RETENÇÃO E ELIMINAÇÃO - IPARATYH EMPREENDIMENTOS IMOBILIARIOS LTDA (FIX URBANISMO)

Código:	PO SGPDP
Versão:	1.0
Data da versão:	01/12/2021
Criado por:	RMSA
Aprovado por:	Comitê de Privacidade
Nível de confidencialidade:	Interno

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
01/12/2021	1.0	RMSA	Elaboração documento

POLÍTICA DE RETENÇÃO E ELIMINAÇÃO - IPARATYH EMPREENDIMENTOS IMOBILIARIOS LTDA (FIX URBANISMO)

INTRODUÇÃO

A FIX URBANISMO deve preservar a segurança e a rastreabilidade de suas informações, bem como a manutenção de todos e quaisquer documentos que possam ser relevantes para eventuais investigações ou defesa de direitos.

Diante disso, elaborou sua Política de Retenção e Eliminação de Documentos com o objetivo de traçar diretrizes quanto à temporalidade da retenção dos documentos em que estejam inclusos dados pessoais, bem como a análise de bases legais para sua manutenção e formas de eliminação.

1. FINALIDADE, ÂMBITO E DESTINATÁRIOS

Esta Política define os períodos de retenção necessários para categorias específicas de dados pessoais e define os padrões mínimos a serem aplicados na destruição de informações que contenham dados pessoais dentro da FIX URBANISMO.

A presente Política de Retenção e Eliminação de Documentos destina-se a todos os sócios, diretores, colaboradores, contratados, consultores e prestadores de serviço que possam recolher, processar ou ter acesso aos dados pessoais controlados pela empresa, independentemente dos meios utilizados para sua produção, reprodução, aquisição, emprego, armazenamento, recuperação, divulgação, comunicação e eliminação.

A Política abrange endereços eletrônicos, documentos impressos e digitais, imagens e áudio, dados gerados por controle de ponto e qualquer outro meio de armazenamento de dados pessoais disponibilizado à execução de seus negócios.

A finalidade da presente Política é que as orientações quanto a retenção e descarte de documentos estejam em conformidade à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), bem como atendam ao princípio da finalidade e minimização dos dados, no que se refere ao armazenamento, descarte e eliminação de dados pessoais de arquivos físicos e digitais mantidos pela FIX URBANISMO.

2. MEIOS DE COLETA E ARMAZENAMENTO

O armazenamento de dados pessoais é feito pela FIX URBANISMO tanto de forma digital quanto de forma física. Para atender às demandas da organização, os documentos são armazenados nos seguintes locais:

(i) Servidor local;

(ii) Website: https://www.fixurbanismo.com.br/

(iii) Arquivos físicos;

(iv) Plataformas e sistemas eletrônicos de gestão;

3. RETENÇÃO DOS DADOS ARMAZENADOS

De acordo com o Laudo de Inventário da FIX URBANISMO, os dados pessoais serão tratados durante o período necessário para atingir os objetivos de seu tratamento, inclusive considerando o prazo e limitações enquanto operadora dos dados dos contratantes (empreendimentos), da seguinte forma:

- Se o tratamento de dados pessoais for necessário para a execução de um contrato – até a rescisão do contrato ou prazo estipulado no mesmo e, em seguida ao término, em período exigido em regulamentação pertinente;
- Se o tratamento for necessário para o cumprimento de uma obrigação legal a qual a FIX URBANISMO esteja sujeita devido às suas atividades e execução de seus contratos – quando tais obrigações forem cumpridas pela organização;
- Se o tratamento for baseado no consentimento explícito do titular – imediatamente após sua solicitação para que os dados sejam eliminados, nos momentos em que os interesses legítimos prosseguidos pela FIX URBANISMO forem cumpridos ou até o momento em que o titular dos dados pessoais tiver recusado o tratamento, exceto em caso de motivos legítimos para o tratamento adicional dos dados.

Sendo assim, ultrapassado o prazo de guarda de documentos que envolvam dados pessoais, orienta-se que estes sejam eliminados conforme as recomendações sugeridas nesta Política, em observância à seguinte tabela de temporalidade:

TABELA DE TEMPORALIDADE	
TIPO DE DOCUMENTO	TEMPO DE GUARDA
Documentos tributários	05 ANOS
Contratos no geral	10 ANOS
Relações de trabalho	05 ANOS APÓS FINDA A RELAÇÃO DE TRABALHO OU 02 ANOS APÓS O TÉRMINO DO VÍNCULO EMPREGATÍCIO, NOS CASOS EM QUE NÃO HOUVER O AJUIZAMENTO DE RECLAMATÓRIA TRABALHISTA
Documentos previdenciários	10 ANOS
Contratos de seguro	01 ANO
Instrumento público ou particular que enseje na cobrança de dívidas líquidas	05 ANOS
FGTS	30 ANOS (DEPOSITADO ATÉ NOVEMBRO DE 2014); DEPOSITADO APÓS ESSA DATA, 05 ANOS

3.1. Orienta-se que a FIX URBANISMO realize análise periódica dos arquivos de documentos que envolvam dados pessoais (clientes, corretores, fornecedores, funcionários, etc), no mínimo de seis em seis meses, de modo que seja possível a verificação dos prazos de guarda, conforme tabela acima.

3.2. Constatado que o prazo máximo de armazenamento foi atingido, orienta-se que a informação seja repassada ao Comitê de Privacidade para que possa prosseguir com a eliminação dos dados, conforme diretrizes da presente Política.

3.3. Em caso de solicitação de eliminação feita pelos titulares, esta deve ser analisada pelo Comitê de Privacidade, nos termos da Política de Atendimento aos Titulares e com observância aos prazos de guarda delineados na tabela acima.

3.4. Após análise recorrente dos arquivos pelo Comitê de Privacidade, os documentos cuja data de armazenamento ultrapasse o prazo de guarda legal disposto na tabela poderão ser mantidos na base de dados da organização, nos casos em que for verificada a existência de outra justificativa e base legal para seu armazenamento.

As bases legais que permitem a manutenção dos arquivos são as seguintes:

- cumprimento de contrato (inciso V do artigo 7º da Lei nº 13.709/18);
- obrigação legal ou regulatória (inciso II do artigo 7º da Lei nº 13.709/18);
- legítimo interesse (inciso IX do artigo 7º da Lei nº 13.709/18);
- consentimento (inciso I do artigo 7º da Lei nº 13.709/18);
- exercício regular de direitos em processo judicial, administrativo ou arbitral (inciso VI do artigo 7º da Lei nº 13.709/18);

3.5. Orienta-se que, previamente ao descarte programado, o Comitê de Privacidade solicite ao departamento jurídico informações quanto a pendências judiciais e/ou administrativas existentes e em curso, em que haja necessidade da manutenção de algum dos respectivos documentos para efeitos de prova.

3.6. Não havendo outra justificativa e base legal para a manutenção dos documentos e tratamento dos dados pessoais ali dispostos, estes obrigatoriamente deverão ser eliminados.

4. *BACKUP* DOS DADOS DURANTE O PERÍODO DE RETENÇÃO

A possibilidade de que os meios de dados usados para *backup* se desgastem deve ser considerada. Se forem escolhidos meios de *backup* eletrônicos, todos os procedimentos e sistemas que garantem o acesso à informação durante o período de retenção (tanto no que diz respeito ao portador da informação quanto a legibilidade dos formatos) também serão

guardados de maneira a proteger as informações contra perdas como resultado de futuras mudanças tecnológicas. A responsabilidade pelo armazenamento é de todos, seguindo as orientações dispostas na Política Interna de Segurança da Informação.

Deverão existir controles apropriados que impeçam a perda permanente de informações essenciais da empresa como resultado da destruição maliciosa ou não intencional de informações – controles estes, descrito na Política Interna de Segurança da Informação.

5. ELIMINAÇÃO DE DOCUMENTOS

A organização e seus colaboradores, em auxílio ao Comitê de Privacidade, devem regularmente rever todos os documentos contendo dados pessoais que estejam sob sua guarda e controle, sejam eles mantidos eletronicamente ou em papel, para decidir eliminar ou excluir quaisquer dados, quando a finalidade para a qual esses documentos foram criados já não é mais relevante, o tempo de guarda se encontre expirado e não haja base legal que justifique sua manutenção.

Uma vez tomada a decisão pela eliminação, os dados devem ser excluídos, triturados ou destruídos tendo em atenção se é papel ou em formato eletrônico, dependendo da sua forma e tendo em conta sempre o grau equivalente ao seu valor e o seu nível de confidencialidade.

O método de destruição varia e depende da natureza do documento. Em particular, quaisquer documentos que contenham informações sensíveis ou confidenciais devem ser destruídos como lixo confidencial e estar sujeitos à eliminação eletrônica segura.

5.1. ELIMINAÇÃO DE ARQUIVOS FÍSICOS

5.1.1. Recomenda-se a designação de um colaborador como responsável pelo processo de descarte, devendo executar a tarefa e assumir as responsabilidades relevantes para a destruição da informação de forma adequada, nos termos da Lei Geral de Proteção de Dados e outras Políticas internas vigentes na organização.

5.1.2. Em momento anterior ao descarte, devem-se tornar ilegíveis todos os documentos físicos, utilizando, por exemplo, os seguintes meios:

a) Triturador de papéis; ou

b) Incinerador de papéis.

5.2. ELIMINAÇÃO DE ARQUIVOS DIGITAIS

5.2.1. Recomenda-se que os arquivos digitais selecionados para descarte, bem como todas as suas cópias, incluindo cópias de segurança (*backup*), sejam deletados e eliminados de forma a impossibilitar a recuperação posterior de quaisquer arquivos eliminados;

5.2.2. Caso a organização opte por não descartar os respectivos arquivos digitais, estes devem ser anonimizados com técnicas específicas, de modo que garanta a segurança desses arquivos e a impossibilidade de associação dos dados ao seu titular, como por exemplo:

a) Generalização de dados;

b) Adição de ruídos à dados; ou

c) Criptografia*.

* CRIPTOGRAFIA: Deverá observar os melhores padrões de mercado e razoáveis ao nível de confidencialidade do documento, sendo sugerida a adoção, minimamente dos seguintes padrões, que devem ser avaliados e confirmados pela TI: I. Os encriptadores em utilização devem atender ou superar os requisitos definidos como "AES-compatíveis" ou "parcialmente AES-compatíveis" de acordo com: o "Catálogo de cifras do IETF/IRTF"; os definidos para utilização pelo National Institute of Standards and Technology (NIST) na publicação FIPS 140-2 ou outra publicação mais atualizada, dependendo da data da implementação. II. A utilização do padrão AES (Advanced Encryption Standard) é altamente recomendada para criptografia simétrica. Recomenda-se fortemente a utilização dos algoritmos RSA e ECC (Elliptic Curve Cryptography) para criptografia assimétrica.

6. LISTAGEM DE ELIMINAÇÃO

6.1. O colaborador ou empresa prestadora de serviço que ficar responsável pelo descarte seguro e confiável, tanto dos arquivos físicos quanto dos arquivos digitais, deverá listar os documentos a serem descartados, registrando todo o processo aplicado para seu arquivo.

6.2. A respectiva lista de eliminação deve ser repassada ao Comitê de Privacidade previamente ao descarte. Nela serão preenchidas a data da autorização para eliminação dos documentos ou anonimização dos dados, bem como coletadas as assinaturas dos membros do Comitê de Privacidade, comprovando sua ciência quanto ao descarte.

6.3. Todo o processo de eliminação deverá ser formalmente documentado e devidamente aprovado o processo de destruição. Assim, serão registrados também os requisitos legais para destruição de informações, particularmente os prazos dispostos na Tabela do item 4 e demais requisitos aplicáveis à integral observância da LGPD.

7. DIRETRIZES COMPLEMENTARES:

7.1. A FIX URBANISMO deve promover entre os colaboradores a conscientização sobre a gestão de documentos de modo a orientá-los que sejam preservados documentos relevantes em meio físico ou eletrônico, enquanto não autorizado formalmente o descarte.

7.2. Deve-se alertar os Gestores da Informação que microcomputadores e *notebooks* corporativos, assim como dispositivos móveis, caso existam, só poderão ser formatados, se preservarem todos e quaisquer documentos que nele estejam armazenados e que possam ser relevantes para eventuais investigações.

7.3. Equipamentos eletrônicos que apresentarem defeito deverão ser previamente avaliados de maneira criteriosa pela área de Tecnologia da Informação, a qual verificará se a formatação é a única alternativa para o reparo do equipamento.

7.4. Os equipamentos que não tiverem autorização para formatação deverão ter seus discos rígidos substituídos e os originais preservados em local seguro e, caso solicitado, disponibilizados para o Departamento Interno interessado, após autorização do Comitê de Privacidade.

7.5. Na impossibilidade técnica de remoção do disco rígido, todo o equipamento deverá ser preservado.

7.6. Em caso de dúvida sobre a retenção de informações, o colaborador deve entrar em contato com o superior hierárquico ou responsável pela proteção de dados para obter orientação antes de tomar qualquer providência, uma vez que a exclusão, dano ou modificação de documentos contendo dados pessoais, mesmo que inadvertidamente, poderá gerar consequências negativas à FIX URBANISMO e a seus colaboradores, segundo os atos normativos vigentes.

8. CONSIDERAÇÕES FINAIS:

8.1. Qualquer suspeita de violação da presente Política deve ser imediatamente reportada ao Comitê de Privacidade.

8.2. Para que os propósitos pretendidos com a presente Política sejam devidamente alcançados, todas as áreas diretamente envolvidas com o tratamento de documentos que contenham dados pessoais deverão atuar em conjunto, com o propósito de mitigar riscos legais e administrativos envolvendo a retenção indevida de dados ou sua eliminação maliciosa.

8.3. Esta Política entra em vigor a partir da data de sua aprovação pelo Comitê de Privacidade, sendo que seu cumprimento fortalece os alicerces e consolida a cultura de privacidade presente em toda FIX URBANISMO.

ATENÇÃO:
Nos casos em que a Fix for apenas Operadora dos dados pessoais, ela deverá observar as orientações previstas nos contratos com seus contratantes para devolução ou eliminação de dados pessoais

VISTO COMITÊ DE PRIVACIDADE:

FIX
URBANISMO