

POLÍTICA CORPORATIVA DE PRIVACIDADE DE DADOS – MONCALIERICAPITAL

1. Objetivo

A presente Política de Privacidade de Dados tem como objetivo estabelecer diretrizes e responsabilidades para o tratamento adequado de dados pessoais pela MONCALIERICAPITAL. Busca assegurar a proteção da privacidade dos titulares, em conformidade com a Lei nº 13.709/2018 (LGPD) e demais normativos aplicáveis. As diretrizes contidas nesta política são de observância obrigatória para todos os colaboradores e terceiros envolvidos com o tratamento de dados pessoais na MoncalieriCapital. A política visa orientar todos os setores da empresa a adotarem práticas transparentes e seguras no tratamento de dados pessoais, em consonância com as melhores práticas de mercado e exigências regulatórias.

2. Escopo

Esta política aplica-se a todas as atividades da MoncalieriCapital que envolvam o tratamento de dados pessoais, abrangendo todas as unidades de negócio, departamentos, sistemas e processos da empresa. Inclui quaisquer formas de coleta, armazenamento, uso, compartilhamento e descarte de dados pessoais de clientes, colaboradores, fornecedores e demais titulares sob responsabilidade da MoncalieriCapital. A abrangência da política contempla todas as unidades organizacionais, sistemas e canais de comunicação da MoncalieriCapital, inclusive serviços de nuvem e operações terceirizadas de processamento de dados.

3. Fundamentos normativos e doutrinários

A MoncalieriCapital fundamenta sua política nas principais normas e diretrizes legais de proteção de dados, notadamente na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e no Marco Civil

da Internet (Lei nº 12.965/2014). Observa ainda as orientações de órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD) e o Banco Central do Brasil. Adotam-se como referência também as melhores práticas previstas em normas internacionais, tais como ISO/IEC 27001 e ISO/IEC 27701, além das diretrizes setoriais aplicáveis ao setor financeiro.

4. Princípios da privacidade e proteção de dados (art. 6º da LGPD)

A MoncalieriCapital adota como pilares os princípios estabelecidos no art. 6º da LGPD, os quais devem nortear todo tratamento de dados pessoais realizado pela empresa:

- ✓ Finalidade: Tratamento de dados para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de uso incompatível com essas finalidades.
- ✓ Adequação: Compatibilidade do tratamento com a finalidade informada ao titular, de acordo com o contexto do serviço prestado.
- ✓ Necessidade: Limitação do tratamento ao mínimo necessário para o cumprimento de suas finalidades, evitando a coleta de dados excessivos ou irrelevantes.
- ✓ Livre acesso: Garantia ao titular de consulta facilitada aos seus dados, assim como às informações sobre o tratamento realizado.
- ✓ Qualidade dos dados: Manutenção de dados pessoais exatos, claros, pertinentes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento.
- ✓ Transparência: Disponibilização de informações claras, precisas e de fácil acesso sobre as formas de tratamento de dados e os agentes envolvidos, resguardados os segredos comercial e industrial.

- ✓ Segurança: Implementação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- ✓ Prevenção: Adoção de ações para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
- ✓ Não discriminação: Vedação ao tratamento de dados para finalidades discriminatórias ilícitas ou abusivas.
- ✓ Responsabilização e prestação de contas: Demonstração contínua pela empresa da adoção de medidas eficazes que comprovem a observância e a conformidade com as normas de proteção de dados, respondendo por quaisquer incidentes ou descumprimentos.

5. Tipos de dados coletados e finalidade

A MoncalieriCapital coleta apenas dados pessoais adequados, relevantes e limitados às finalidades informadas. Entre os principais tipos de dados coletados estão:

- ✓ Dados cadastrais e identificadores (por exemplo, nome, CPF, RG, data de nascimento, endereço, documentos de identificação) para abertura de contas, cadastro de clientes e cumprimento de obrigações contratuais e regulatórias.
- ✓ Dados de contato e comunicação (e-mail, telefone, endereço postal) para envio de notificações, atualizações contratuais, avisos de segurança, suporte e atendimento ao cliente.
- ✓ Dados financeiros e transacionais (informações bancárias, histórico de transações, faturas) para análise de crédito, prevenção a fraudes, auditoria financeira e execução dos serviços de pagamento contratados.

- ✓ Dados de uso e contexto (registros de acesso aos sistemas, endereços IP, logs de atividade, dados de localização) para monitoramento de segurança, solução de problemas técnicos e melhoria de serviços.
- ✓ Dados sensíveis (como origem racial, convicções religiosas, dados de saúde, orientação sexual, biometria etc.) somente quando indispensáveis às finalidades específicas, com base legal apropriada e observando as exigências de segurança previstas em lei.
- ✓ Dados de colaboradores e prestadores de serviços (informações cadastrais, contratuais, profissionais e bancárias) para fins de gestão de recursos humanos, folha de pagamento e cumprimento de obrigações trabalhistas, fiscais e previdenciárias.

Cada categoria de dados é coletada para finalidades específicas, que podem incluir: execução de contratos de serviços financeiros, atendimento a obrigações legais e regulatórias, prevenção e detecção de fraudes, marketing autorizado pelo titular, análise estatística, melhorias de produtos, entre outras. A empresa não coleta dados pessoais desnecessários para suas atividades e evita o armazenamento de informações que não tenham finalidade legítima.

6. Bases legais para o tratamento (art. 7º da LGPD)

Os tratamentos de dados pessoais pela MoncalieriCapital são realizados mediante fundamentos jurídicos adequados, de acordo com o art. 7º da LGPD. Entre as bases legais aplicáveis destacam-se:

- ✓ Consentimento do titular (Art. 7º, I): quando o titular autoriza livre, informado e expressamente o tratamento de seus dados para finalidades específicas.
- ✓ Cumprimento de obrigação legal ou regulatória (Art. 7º, II): tratamento necessário para atender às exigências de lei ou

regulamento, tais como obrigações fiscais, trabalhistas, de segurança financeira, de prevenção à lavagem de dinheiro, entre outras.

- ✓ Execução de políticas públicas (Art. 7º, III): nos casos em que haja demanda do Poder Público, conforme previsto em lei, para a execução de políticas públicas.
- ✓ Estudos por órgão de pesquisa (Art. 7º, IV): tratamento para realização de estudos por órgão de pesquisa, assegurando, sempre que possível, a anonimização dos dados.
- ✓ Execução de contrato (Art. 7º, V): tratamento necessário para cumprimento de contrato ou de procedimentos preliminares relacionados a contrato dos quais o titular seja parte (por exemplo, prestação de serviços financeiros).
- ✓ Exercício regular de direitos (Art. 7º, VI): tratamento para exercício regular de direitos em processos judiciais, administrativos ou arbitrais, conforme previsto em lei.
- ✓ Proteção da vida ou da incolumidade física (Art. 7º, VII): tratamento necessário para proteger a vida ou a segurança do titular ou de terceiros.
- ✓ Tutela da saúde (Art. 7º, VIII): tratamento exclusivo em procedimento realizado por profissionais ou serviços de saúde, em contexto de assistência à saúde.
- ✓ Interesse legítimo do controlador (Art. 7º, IX): tratamento para atender interesses legítimos da MoncalieriCapital ou de terceiros (por exemplo, prevenção a fraudes), exceto quando prevalecerem direitos fundamentais do titular que exijam proteção dos dados.

- ✓ Proteção do crédito (Art. 7º, X): tratamento necessário para proteção do crédito do titular, em conformidade com a legislação pertinente (por exemplo, comunicação a órgãos de proteção ao crédito).

Cada operação de tratamento será justificada com uma ou mais dessas bases legais, conforme o caso concreto, e deverá estar documentada de forma transparente. Quando o fundamento for o consentimento, este será obtido de forma expressa e documentada, estando o titular ciente de seus direitos, inclusive de que poderá revogá-lo a qualquer tempo.

7. Direitos dos titulares (art. 18 da LGPD)

A MoncalieriCapital reconhece e assegura aos titulares de dados pessoais os direitos previstos no art. 18 da LGPD. São assegurados aos titulares, mediante requisição dirigida à empresa, entre outros:

- ✓ Confirmação da existência de tratamento: direito de saber se seus dados estão sendo processados pela MoncalieriCapital.
- ✓ Acesso aos dados pessoais: direito de obter cópia dos dados pessoais que a empresa possui sobre o titular.
- ✓ Correção de dados: direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.
- ✓ Anonimização, bloqueio ou eliminação: direito de requerer a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desacordo com a legislação.
- ✓ Portabilidade dos dados: direito de receber os dados em formato estruturado e transmiti-los a outro fornecedor de serviço ou produto, em conformidade com regulamentação da ANPD, observados os segredos comercial e industrial.

- ✓ Eliminação de dados tratados com consentimento: direito de solicitar a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (por exemplo, para cumprimento de obrigação legal ou arquivamento judicial).
- ✓ Informação sobre compartilhamento: direito de ser informado sobre as entidades públicas e privadas com as quais a empresa compartilhou seus dados pessoais.
- ✓ Possibilidade de não consentir: direito de ser informado sobre a possibilidade de não fornecer consentimento e as consequências da recusa.
- ✓ Revogação do consentimento: direito de retirar o consentimento dado anteriormente, sem prejuízo da adoção de outras bases legais para o tratamento, quando aplicáveis.

Os titulares poderão exercer seus direitos gratuitamente, por meio dos canais disponibilizados pela MoncalieriCapital. Respostas às solicitações serão fornecidas em prazo compatível com a legislação e orientações da ANPD, sem custos para o titular.

8. Compartilhamento com terceiros e operadores

A MoncalieriCapital pode compartilhar dados pessoais com terceiros observando sempre a legalidade, a finalidade e a segurança no tratamento. O compartilhamento será feito nas seguintes circunstâncias:

- ✓ Órgãos públicos e autoridades competentes: quando exigido por lei, determinação judicial ou requisição de autoridade regulatória, para cumprimento de obrigações legais, investigações ou processos.
- ✓ Prestadores de serviços e parceiros comerciais: compartilhamento com operadores e subcontratados que realizam atividades de

suporte ou execução de parte das operações da empresa, tais como provedores de tecnologia, processadores de pagamento, instituições de análise de crédito, serviços de nuvem, entre outros. Esses agentes são contratados mediante acordos que impõem obrigações estritas de confidencialidade, segurança e observância das normas de proteção de dados, limitando o uso dos dados às finalidades autorizadas pela MoncalieriCapital.

- ✓ Demais controladores de dados: quando necessário para a execução de contratos ou prestação de serviços de interesse do titular, desde que haja base legal adequada (por exemplo, consentimento específico do titular ou interesse legítimo fundamentado).

Em qualquer compartilhamento, a MoncalieriCapital observa os princípios da LGPD e mantém registros das operações realizadas. A empresa não comercializa dados pessoais dos titulares nem os utiliza para finalidades diversas daquelas autorizadas ou previstas em lei.

9. Transferência internacional de dados

A transferência internacional de dados pessoais para outros países ou organismos internacionais ocorrerá somente nas hipóteses previstas pela LGPD. Em especial, serão observadas as seguintes condições:

- ✓ Nível de proteção adequado: transferência para países reconhecidos pela ANPD como detentores de nível adequado de proteção de dados, em consonância com tratados internacionais ou decisões específicas.
- ✓ Garantias contratuais: adoção de instrumentos contratuais que assegurem salvaguardas adequadas (como cláusulas-padrão de proteção de dados aprovadas pela ANPD, conforme art. 33).
- ✓ Autorizações legais: casos em que a LGPD permite a transferência independentemente de consentimento ou adequação, como

cumprimento de obrigação legal ou regulatória no Brasil, proteção da vida do titular ou de terceiros, ou exercício de direitos contratados.

- ✓ Consentimento específico: nos demais casos, realização de transferência mediante consentimento explícito e destacado do titular, atendidas as condições legais.

A MoncalieriCapital se compromete a assegurar que qualquer transferência internacional atenda rigorosamente aos requisitos da LGPD, especialmente no que tange à segurança e à continuidade da proteção dos direitos do titular nos termos dos arts. 33 a 36 da lei.

10. Retenção e descarte de dados

Os dados pessoais sob responsabilidade da MoncalieriCapital são retidos apenas pelo período estritamente necessário para o cumprimento da finalidade pela qual foram coletados, observando as exigências legais e regulatórias aplicáveis. Os prazos de retenção variam conforme a categoria de dados e são definidos em tabela interna gerida pela área de Compliance.

Findo o prazo de retenção ou a finalidade do tratamento, os dados serão eliminados de forma segura, mediante procedimentos técnicos que impeçam a sua recuperação, ou anonimizados permanentemente para uso em análises estatísticas e estudos, quando permitido.

O processo de descarte seguro inclui a eliminação lógica com sobrescrita de dados e, no caso de suportes físicos, trituração ou destruição segura conforme normas técnicas aplicáveis (p. ex. ABNT NBR ISO/IEC 27040).

11. Segurança e confidencialidade

A MoncalieriCapital adotará todas as medidas técnicas e administrativas necessárias para proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. As diretrizes de segurança incluem:

- ✓ Controles de acesso: restrição do acesso aos sistemas e bancos de dados contendo dados pessoais somente a profissionais autorizados, mediante autenticação robusta e de acordo com o princípio do menor privilégio.
- ✓ Criptografia e proteções técnicas: uso de criptografia, firewalls, VPN e demais recursos tecnológicos de segurança para proteger informações em trânsito e em repouso.
- ✓ Segurança de infraestrutura: manutenção de ambiente de TI seguro (servidores, nuvem, dispositivos móveis) de acordo com as melhores práticas do mercado (ISO/IEC 27001) e com requisitos regulatórios do Banco Central, assegurando confidencialidade, integridade e disponibilidade dos dados.
- ✓ Classificação e segregação de dados: identificação do grau de sensibilidade das informações e adoção de tratamento diferenciado para dados sensíveis e estratégicos.
- ✓ Proteção física: controle de acesso físico a instalações onde estejam armazenados arquivos ou equipamentos que tratam dados pessoais.
- ✓ Treinamento de pessoal: as equipes envolvidas recebem orientação contínua sobre segurança da informação, privacidade de dados e obrigações contratuais e legais relativas à confidencialidade.

- ✓ Planos de contingência: elaboração de planos de resposta a incidentes de segurança, planos de backup e recuperação de desastres, visando à continuidade dos serviços.

Todos os colaboradores e prestadores de serviço da MoncalieriCapital têm obrigação de manter em confidencialidade as informações a que tenham acesso, sob pena de sanções disciplinares. Políticas internas, testes de segurança e auditorias periódicas são realizados para verificar a eficácia das medidas de segurança da informação.

12. Estrutura organizacional de privacidade

A governança de dados pessoais da MoncalieriCapital é sustentada por uma estrutura organizacional clara, com funções e responsabilidades definidas para cada área:

- ✓ Diretoria Executiva: aprova a Política de Privacidade de Dados, aloca recursos necessários e promove uma cultura de conformidade e privacidade em toda a empresa.
- ✓ Encarregado (DPO): coordena a governança de dados pessoais, atuando como facilitador entre as áreas internas, titulares e autoridades; conduz avaliações de conformidade com a LGPD e orienta a implementação das medidas de proteção.
- ✓ Segurança da Informação e TI: responsáveis pela arquitetura e operação dos sistemas de informação, implementam controles técnicos (criptografia, firewalls, autenticação) e mantêm a infraestrutura segura, baseando-se em padrões ISO/IEC 27001/27701.
- ✓ Jurídico/Compliance: presta consultoria jurídica quanto aos aspectos regulatórios de proteção de dados, elabora e revisa contratos (assegurando cláusulas de privacidade e proteção de dados pessoais), acompanha alterações legislativas e garante

que as ações da empresa estejam alinhadas com normas setoriais do Banco Central e orientações da ANPD.

- ✓ Marketing e Desenvolvimento de Produtos: incorporam o princípio de privacy by design nas iniciativas de marketing e no desenvolvimento de produtos/serviços, garantindo a obtenção de consentimento quando necessário, transparência nas comunicações e mínima coleta de dados.
- ✓ Recursos Humanos: gerencia os dados pessoais dos colaboradores da empresa, assegurando o cumprimento da legislação trabalhista e de privacidade; promove treinamentos periódicos sobre proteção de dados e segurança da informação para todos os funcionários.
- ✓ Outras áreas operacionais (como Atendimento, Operações, Financeiro, Auditoria Interna): aplicam as orientações desta política em seus processos internos, contribuindo para a gestão adequada de dados pessoais em todas as fases de suas atividades.

Cada área deve desempenhar seu papel de forma coordenada, sob supervisão do DPO, garantindo que as práticas de tratamento de dados estejam integradas às atividades cotidianas da MoncalieriCapital.

13. Ciclo de vida dos dados (coleta, uso, retenção, eliminação)

A MoncalieriCapital gerencia o ciclo de vida dos dados pessoais por meio de processos definidos que asseguram o tratamento adequado em todas as fases:

- ✓ Coleta: os dados são obtidos diretamente do titular ou de fontes autorizadas, sempre com transparência quanto à finalidade. São adotadas políticas para captar apenas os dados estritamente necessários, com consentimento prévio quando exigido por lei.

- ✓ Uso e processamento: os dados coletados são utilizados internamente apenas para as finalidades declaradas. O acesso às informações é restrito a profissionais autorizados e as atividades de tratamento (como análise, compartilhamento ou processamento em sistemas) são auditadas. Quaisquer novas utilizações dos dados que não tenham previsão legal ou contratual exigirão reavaliação da base legal.
- ✓ Armazenamento e retenção: os dados são armazenados em ambientes controlados, com mecanismos de segurança. São mantidos pelo tempo necessário para cumprir suas finalidades e atender às obrigações legais aplicáveis. Durante esse período, backups regulares e registros de logs garantem a integridade e disponibilidade das informações.
- ✓ Eliminação ou anonimização: ao final do prazo de retenção ou quando cessar a necessidade do tratamento, os dados serão eliminados de forma segura ou anonimizados permanentemente. Processos de anonimização são empregados sempre que viável, permitindo a utilização de dados sem identificação dos titulares em análises futuras.

Esse ciclo de vida é documentado e revisado regularmente, de modo a incorporar melhorias e atender a novos requisitos normativos e de segurança.

14. Gestão de consentimento e revogação

A gestão de consentimento é realizada de forma estruturada e transparente. Em situações em que o tratamento de dados pessoais exige consentimento, a MoncalieriCapital adota as seguintes práticas:

- ✓ Obtenção do consentimento: coleta-se o consentimento de forma clara, inequívoca e destacada, informando ao titular sobre a finalidade específica do tratamento e seu direito de

revogação. Os consentimentos são registrados eletronicamente ou por escrito, garantindo evidências em conformidade com as normas aplicáveis.

- ✓ Gerenciamento de registros de consentimento: mantém-se um sistema eletrônico para registrar a data, forma e escopo do consentimento obtido, permitindo auditoria e verificação futura. Somente os dados cujos titulares consentiram são tratados nos casos em que essa seja a base legal escolhida.
- ✓ Revogação do consentimento: o titular tem o direito de retirar o consentimento a qualquer tempo. A MoncalieriCapital disponibiliza meios simples para essa revogação, processando-a sem ônus para o titular. Após a revogação, o tratamento de dados somente continuará se houver outra base legal aplicável ou obrigações legais que impeçam sua exclusão imediata.
- ✓ Consentimento para compartilhamento entre controladores: quando o tratamento inicial dos dados ocorreu sob consentimento do titular e for necessária a transferência ou compartilhamento desses dados com outro controlador, a MoncalieriCapital buscará novo consentimento específico para essa finalidade, conforme exigido pela legislação.

Esses procedimentos garantem que o consentimento seja administrado de forma consistente e que os titulares possam exercer controle sobre seus dados pessoais ao longo do relacionamento com a MoncalieriCapital.

15. Registro de operações de tratamento (ROPA) e Medidas de Anonimização e Pseudonimização

Conforme art. 37 da LGPD, a MoncalieriCapital mantém um Registro de Operações de Tratamento de Dados Pessoais (ROPA) completo. Esse

registro contém informações essenciais sobre os tratamentos realizados, tais como:

- ✓ Finalidade de cada operação de tratamento;
- ✓ Categoria dos titulares (clientes, colaboradores, fornecedores etc.) e tipos de dados pessoais envolvidos;
- ✓ Bases legais aplicáveis a cada tratamento;
- ✓ Operadores e subcontratados que acessam ou processam os dados;
- ✓ Descrição de eventual compartilhamento de dados com terceiros;
- ✓ Prazo de retenção estimado ou critérios para descarte;
- ✓ Medidas de segurança adotadas em cada etapa.

O ROPA é gerenciado pelo Encarregado de Dados (DPO) em conjunto com as áreas responsáveis por cada processo de negócio. É revisado periodicamente e atualizado sempre que ocorrer qualquer mudança relevante nos processos de tratamento. Esse registro serve como ferramenta de governança interna e está disponível para auditorias e fiscalizações pela ANPD e demais autoridades competentes.

A MoncalieriCapital adota, sempre que possível, técnicas de anonimização e pseudonimização para reduzir os riscos associados ao tratamento de dados pessoais. Essas medidas visam proteger a identidade dos titulares, especialmente em contextos de análise estatística, teste de sistemas e pesquisa.

Anonimização: técnica que remove a possibilidade de associação direta ou indireta entre os dados e o titular, de forma irreversível, conforme definido pela LGPD. Dados anonimizados não são considerados dados pessoais e podem ser utilizados para fins legítimos como estatísticas e melhoria de produtos.

Pseudonimização: técnica que substitui identificadores diretos por códigos ou chaves reversíveis, restringindo o acesso aos dados originais apenas a pessoas autorizadas. Essa prática é aplicada especialmente em ambientes de teste, backups e fluxos internos com menor necessidade de identificação direta do titular.

A adoção dessas medidas é avaliada caso a caso, levando em conta o tipo de dado, a finalidade do tratamento e os riscos à privacidade dos titulares.

16. Avaliação de impacto (DPIA) e mitigação de riscos

Para tratamentos que envolvam alto risco à privacidade dos titulares, a MoncalieriCapital realiza análise prévia e, quando necessário, Avaliação de Impacto à Proteção de Dados (DPIA), conforme previsto nos arts. 38 e 39 da LGPD. Esse processo inclui:

- ✓ Identificação de riscos: análise das operações de tratamento, considerando a sensibilidade dos dados, a escala do processamento e as possíveis consequências para os titulares em caso de incidente ou uso indevido.
- ✓ Realização da DPIA: elaboração de relatório de impacto que descreve os riscos identificados e as medidas existentes para mitigá-los. A DPIA envolve equipes multidisciplinares (negócios, TI, segurança, jurídico).
- ✓ Plano de mitigação: definição e implementação de controles adicionais e ações corretivas para reduzir riscos inaceitáveis, tais como aumento de criptografia, segregação de sistemas, anonimização de dados e restrições adicionais de acesso.
- ✓ Monitoramento contínuo: acompanhamento dos riscos ao longo do tempo, com atualização periódica da DPIA quando houver mudanças significativas no tratamento de dados ou no ambiente regulatório.

A empresa documenta todas as etapas do processo de avaliação de impacto e garante a efetividade das medidas mitigadoras, revisando-as sempre que novas vulnerabilidades sejam identificadas ou novas exigências legais sejam impostas.

17. Gestão de fornecedores (contratos com cláusulas de privacidade)

A MoncalieriCapital adota critérios rigorosos na seleção e gestão de fornecedores que manipulam dados pessoais. As principais práticas incluem:

- ✓ Avaliação pré-contratual: análise da capacidade técnica e jurídica do fornecedor em cumprir requisitos de segurança e privacidade, conforme orientações da Resolução CMN nº 4.893/2021 e da LGPD.
- ✓ Cláusulas contratuais específicas: inclusão obrigatória de cláusulas nos contratos que estabeleçam obrigações de confidencialidade, adoção de medidas de segurança compatíveis (p.ex., conforme normas ISO/IEC 27001/27701), restrição do uso dos dados às finalidades contratadas e notificação imediata de qualquer incidente de segurança envolvendo dados da MoncalieriCapital.
- ✓ Auditoria e monitoramento: procedimentos de auditoria periódica para verificar o cumprimento das obrigações contratuais de proteção de dados pelos fornecedores. Caso sejam identificadas não conformidades, são exigidas ações corretivas imediatas.
- ✓ Revisão de contratos: atualização contratual sempre que houver mudanças nas leis de proteção de dados ou nos serviços prestados, garantindo que novos requisitos (p.ex., comunicação de incidentes à ANPD) sejam cobertos.

- ✓ Essa gestão de fornecedores assegura que terceirizados mantenham padrões de proteção de dados compatíveis com a política da MoncalieriCapital e com o exigido pela legislação.

18. Resposta a incidentes envolvendo dados pessoais e comunicação com ANPD

A MoncalieriCapital possui um Plano de Resposta a Incidentes de Segurança que inclui procedimentos específicos para incidentes que envolvam dados pessoais. Em caso de ocorrência de incidente que possa acarretar risco ou dano relevante aos titulares, são realizadas as seguintes ações:

- ✓ Identificação e contenção: detecção precoce do incidente por meio de monitoramento de segurança e procedimentos de alerta. Imediata contenção do evento para evitar sua expansão.
- ✓ Avaliação e análise: investigação técnica para apurar a natureza, causa e extensão do incidente, incluindo levantamento dos dados afetados e possíveis vulnerabilidades exploradas.
- ✓ Comunicação interna: ativação da equipe de gerenciamento de incidentes (segurança da informação, TI, jurídico, compliance) e comunicação às instâncias decisórias da empresa.
- ✓ Notificação à ANPD e titulares: conforme art. 48 da LGPD, incidente significativo envolvendo dados pessoais será comunicado à Autoridade Nacional de Proteção de Dados e aos titulares impactados. A comunicação será feita em prazo compatível com a gravidade do incidente (seguindo recomendação de até 72 horas após a sua detecção, quando possível), contendo informações sobre a natureza dos dados afetados, as medidas adotadas e orientações para os titulares.
- ✓ Mitigação e correção: implementação de ações corretivas para remediar vulnerabilidades exploradas e prevenção de novos

incidentes, incluindo reforço de medidas de segurança ou revisão de procedimentos.

- ✓ Registro e aprendizado: documentação completa do incidente, lições aprendidas e atualização de políticas e controles para evitar reincidência.

Essa abordagem garante resposta célere e coordenada a incidentes, em conformidade com as exigências legais e regulatórias, minimizando danos aos titulares e à empresa.

19. Treinamento e conscientização dos colaboradores

- ✓ A MoncalieriCapital promove periodicamente programas de formação e sensibilização de todos os colaboradores quanto à proteção de dados pessoais e segurança da informação. As iniciativas incluem:
- ✓ Treinamentos obrigatórios: cursos presenciais e on-line para novos funcionários e atualizações regulares para o quadro existente, abordando conceitos da LGPD, procedimentos de segurança, políticas internas e responsabilidades individuais.
- ✓ Campanhas de conscientização: comunicações internas (e-mails, cartilhas, vídeos) sobre temas como engenharia social, phishing, uso correto de senhas e manuseio de dados sensíveis, reforçando a importância da confidencialidade e do compliance.
- ✓ Simulações e avaliações: realização de testes práticos (por exemplo, simulação de ataques de phishing) para medir o grau de conscientização e adotar medidas corretivas quando necessário.
- ✓ Cultura de privacidade: engajamento de lideranças para disseminar a importância do tratamento adequado de dados pessoais, estimulando a denúncia de práticas inseguras e a

adoção de comportamentos alinhados às melhores práticas de proteção de dados.

Essas ações visam garantir que todos os colaboradores entendam suas responsabilidades, reduzindo riscos internos de violação de dados e fortalecendo a cultura de privacidade na organização.

20. Atualização e revisão periódica

Esta Política Corporativa de Privacidade de Dados será revisada periodicamente ou sempre que ocorrerem alterações significativas no ambiente regulatório, normativo ou nos processos de negócio da MoncalieriCapital.

As atualizações desta política deverão ser aprovadas pela Alta Direção da MoncalieriCapital e comunicadas a todos os colaboradores.

Esta política será revisada anualmente ou sempre que houver alterações significativas no ambiente regulatório, tecnológico ou organizacional.

A MoncalieriCapital promoverá a disseminação desta política por meio de treinamentos periódicos, ações de comunicação interna e disponibilização em repositório acessível a todos os colaboradores. A adesão e compreensão são obrigatórias.

MONCALIERICAPITAL™ Compliance Corporativo. Aprovado em 16/06/2025.