Gávea INVESTIMENTOS

Agosto de 2012

Atualizado em Dezembro de 2021

MANUAL DE COMPLIANCE

Políticas e Procedimentos

POLÍTICAS

14. POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

A Gávea tem a responsabilidade legal e regulatória de proteger a privacidade dos dados pessoais coletados, direta ou indiretamente de todos os indivíduos, incluindo, mas não limitando aos atuais, futuros ou potenciais clientes, parceiros de negócios, colaboradores e outras pessoas identificáveis. Dados pessoais devem ser sempre colocados em áreas seguras e só podem ser compartilhadas com pessoas autorizadas.

O programa de proteção de dados da Gávea visa estabelecer e manter padrões elevados para coletar, usar, divulgar, armazenar, proteger, acessar, transferir ou processar dados pessoais.

A Gávea se utiliza de princípios de privacidade como:

- **Razoabilidade**: Processamento de dados pessoais de forma legal, justa e transparente.
- **Limitação de finalidade**: Dados pessoais somente serão coletados para fins específicos, explícitos e legítimos. Processamentos subsequentes serão compatíveis com tais finalidades, a menos que a Gávea tenha obtido consentimento expresso do Titular do Dado ou o processamento seja feito para o cumprimento das obrigações legais e regulatórias, para o exercício regular de direitos e, quando necessário para a execução de contratos ou para atender a interesses legítimos da Gávea, clientes e terceiros.
- **Proporcionalidade**: Dados serão processados desde que adequados, relevantes e não excessivos para as finalidades nas quais eles são processados.
- **Integridade de dados**: Os dados pessoais deverão ser precisos, completos e atualizados, conforme necessário para as finalidades nas quais eles são processados.
- **Segurança de dados**: A Gávea toma medidas técnicas e organizacionais apropriadas para proteger os Dados pessoais contra alteração ou perda acidental ou ilegal, ou de uso, divulgação ou acesso não autorizado, de acordo com sua política interna.

Em conformidade com a legislação atual, a Gávea garante aos titulares de dados diversos direitos, como:

- **Direito de acesso**: Os titulares de dados podem solicitar a confirmação do tratamento dos dados e ainda o acesso aos seus dados pessoais armazenados pela Gávea. E ainda, podem solicitar a correção de dados pessoais imprecisos ou ter dados pessoais incompletos completados.
- **Direito de revogação do consentimento dado para o tratamento de dados pessoais.**
- **Solicitação de anonimização, bloqueio ou eliminação de dados** desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.
- **Direito de ser esquecido:** Os titulares de dados têm o direito de serem esquecidos, solicitando a exclusão de seus dados pessoais nos casos em que os dados não são mais necessários de acordo com a legislação vigente.
- **Direito de informação** das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados.

Para exercer estes direitos, o Titular do Dado deverá encaminhar sua solicitação para o e-mail do *Data Privacy Officer* (Encarregado) da Gávea (DPO@gaveainvest.com.br).

Em especial, são consideradas confidencias as informações obtidas de clientes (dados pessoais, posições, movimentações, etc.) e também as informações relacionadas às operações dos fundos geridos (posições, risco, decisões de investimento, informações materiais não públicas, etc.). Informações materiais não

públicas relacionadas a companhias abertas devem ser tratadas com o devido cuidado e de acordo com a Política de Prevenção ao Uso de Informação Privilegiada.

Informações pessoais não públicas de clientes incluem qualquer informação: (i) fornecida pelos investidores que buscam obter um produto ou serviço financeiro; (ii) resultante de uma transação de ou com Clientes; e (iii) obtida de outra forma ligada ao fornecimento de um produto ou serviço aos Clientes, tal como informações de um relatório de consumidor ou outra fonte externa usada para verificar informações sobre um Cliente. As informações confidenciais a que a Gávea pode ter acesso incluem, mas não estão limitadas a: (i) nomes de clientes, endereços e números de telefone; (ii) números de identidade e CPF; (iii) situação financeira e de renda; e (iv) participações e posições em nossos fundos de investimento; (v) resultados do *background check*; e (v) reportes de atividades suspeitas.

É dever da Gávea: (i) garantir a segurança e confidencialidade das informações pessoais não públicas; (ii) proteger a segurança de tais informações contra qualquer ameaça ou perigo antecipados; (iii) proteger tais informações contra o acesso ou uso não autorizado; e (iv) garantir a correta eliminação dos dados pessoais em caso de solicitação do Titular dos dados.

Todos os Colaboradores devem manter e preservar a confidencialidade das informações pessoais não públicas confiadas à Gávea. É de absoluta importância que os titulares de dados pessoais saibam que as informações que eles fornecem serão tratadas com integridade e discrição. As informações confidenciais devem ser salvaguardadas para todos os Titulares de Dados.

Informações confidenciais fornecidas, verbalmente ou por meio de documentos, por Cliente que posteriormente decide não iniciar negócios com a Gávea também estão sujeitas a essas políticas e procedimentos e devem ser preservadas com o mesmo cuidado dispensado aos demais Clientes.

A Gávea realiza o tratamento de dados pessoais com finalidades específicas e de acordo com as bases legais previstas na Lei nº 13.709/18, alterada pela Lei 13.853/2019, Lei Geral de Proteção de Dados **("LGPD")**.

Informações pessoais confidenciais podem ser: (i) compartilhadas dentro da Gávea apenas conforme a necessidade de modo a executar os negócios; (ii) compartilhadas com as afiliadas da Gávea e outras firmas – no Brasil e no Exterior - que ajudam a atender o Cliente e necessitam dessas informações tal como um distribuidor (observadas as restrições contratuais para cada caso); e (iii) compartilhada com os reguladores, auto reguladores e/ou quando exigido por lei, norma, regulamentos ou ordem judicial emitida por um tribunal de jurisdição competente, ou por um órgão, judiciário, administrativo ou legislativo; desde que, no entanto, o Comitê de Compliance seja consultado previamente. Quaisquer exceções envolvendo o compartilhamento de informações confidenciais com pessoas não autorizadas deverão ser enviadas ao Comitê de Compliance e informadas aos titulares dos dados. Os Colaboradores devem ser prudentes quando se comunicarem eletronicamente.

Os Colaboradores devem verificar a lista de distribuição antes de enviar documentos confidenciais. Documentos confidenciais também não devem permanecer nas impressoras ou sobre as mesas. Todas as informações confidenciais devem ser colocadas em áreas seguras.

Os Colaboradores devem informar o Comitê de Compliance imediatamente caso tenham conhecimento que informações confidenciais foram acessadas por pessoas não autorizadas.

Com o objetivo de resguardar as informações sigilosas inerentes às atividades da Gávea Investimentos que exigem grau especial de fidúcia, os candidatos a colaboradores – antes de qualquer formalização de contratação – passarão por processo *de background check*.

Informações pessoais confidenciais, incluindo quando for o caso dados sensíveis, dos colaboradores da Gávea e seus dependentes poderão ser compartilhadas com empresas terceiras contratadas pela Gávea para gerir benefícios disponibilizados aos próprios colaboradores para a específica finalidade de concessão dos benefícios, capacitação técnica, integração, fixação de indicadores, metas e cotas, acompanhamento de

desempenho e desenvolvimento de colaboradores, pesquisas de engajamento, pagamento, gestão, regime disciplinar, procedimentos para admissão, movimentações, promoção, estabilidade, afastamento, desligamento e reintegração, cadastros.

Proteção da Informação

A Gávea está comprometida e empenhada em buscar o mais alto grau de proteção de suas informações e sistemas. A Gávea investe em ferramentas e tecnologias para garantir que sua infraestrutura de tecnologia esteja em linha com as melhores práticas em termos de segurança e confiabilidade. Os procedimentos de segurança dos sistemas aplicados pela empresa são revistos continuamente e atualizados sempre que necessário. Periodicamente, são realizados também testes de segurança e treinamentos com os funcionários sobre o uso apropriado da infraestrutura de tecnologia.

As práticas de segurança da informação adotadas pela Gávea têm como objetivo impedir a ocorrência de: (i) transmissão não autorizada de informações confidenciais sobre clientes, Colaboradores ou sobre a Gávea em geral; (ii) cópia ou transmissão não autorizada de softwares ou dados proprietários; (iii) acesso não autorizado a arquivos, comunicações e outros dados confidenciais relacionados aos clientes, Colaboradores da Gávea ou à Gávea em geral; (iv) tentativas de interceptação de e-mail ou mensagem instantânea da Gávea; (v) quaisquer ataques cibernéticos à Gávea; e (vi) liberação não autorizada de senhas e códigos de ID de usuários.

Os privilégios de acesso a sistemas, dados e instalações da Gávea são concedidos aos Colaboradores conforme a necessidade e as atividades desempenhados. Os Colaboradores devem sempre proteger adequadamente suas estações de trabalho, senhas, acessos pessoais e informações confidenciais sob sua responsabilidade e devem utilizar adequada e profissionalmente os recursos da Gávea.

Os colaboradores têm o dever de reportar imediatamente qualquer indício de falha, invasão ou comportamento suspeito dos sistemas da Gávea.

A política de confidencialidade e segurança da informação poderá ser atualizada conforme alterações no escopo de negócios da Gávea ou alterações legais e estará disponível no site da Gávea versão atualizada.

O departamento de Tecnologia é responsável por realizar, periodicamente, testes de segurança e procedimentos para detectar falhas e vulnerabilidades nos sistemas da Gávea. O departamento de Tecnologia é responsável ainda por tomar as medidas cabíveis para avaliar e mitigar os danos em caso de falhas identificadas. Conforme necessário, incidentes relevantes devem ser escalados para os membros do Comitê de *Cybersecurity* para que sejam avaliadas as implicações legais e regulatórias, bem como as ações corretivas apropriadas.