

Brookfield Properties

Programa de Privacidade e Proteção de Dados Pessoais da Brookfield Properties

Fevereiro de 2025

Sumário

1.	Introdução.....	3
2.	Por que a Privacidade e Proteção de Dados Pessoais são tão importantes?3	
3.	Para que serve o Programa?.....	3
3.1.	Vinculação ao Programa da Brookfield Asset Management Inc.....	3
3.2.	Documentos deste Programa.....	4
3.3.	Governança e Liderança pelo Exemplo.....	4
3.4.	Monitoramento de Conformidade.....	4
3.5.	Comunicação e Treinamento.....	4
3.6.	Contatos-Chave.....	5
3.7.	Mudança Regulatória.....	5
4.	Princípios Fundamentais.....	5
5.	<i>Privacy by Design</i>	6
6.	Controle e Histórico de Versões.....	7
7.	Aprovações.....	7
	Anexo A.....	9
	Anexo B.....	10
	Anexo C.....	14

1. Introdução

A Brookfield Properties está comprometida com o cumprimento de todas as exigências legais e regulamentares aplicáveis relacionadas a privacidade e proteção de dados pessoais e, para tanto, considera o tratamento legal e correto dos Dados Pessoais (conforme definição abaixo) como parte integrante de nossas operações.

Este documento descreve o Programa de Privacidade e Proteção de Dados Pessoais da Brookfield Properties Brasil Realty Administrações de Imóveis Ltda. (respectivamente, “Programa” e “Brookfield Properties”) para garantir o cumprimento da legislação aplicável, e em especial, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, doravante denominada “LGPD”).

Este Programa é aplicável a Brookfield Properties, no exercício de suas atividades, bem como aos fundos de investimento e empresas cujos ativos/investimentos estejam sob sua administração (“Fundos” e, em conjunto com Brookfield Properties, apenas “Empresa”).

2. Por que a Privacidade e Proteção de Dados Pessoais são tão importantes?

Os Dados Pessoais são considerados ativos valiosos, devendo ser objeto de Tratamento eficaz, para cumprir os objetivos de negócios, as expectativas dos investidores e funcionários quanto a exatidão e segurança e a conformidade com a LGPD e demais leis de proteção de dados aplicáveis.

A LGPD tem por objetivos, entre outros, garantir boas práticas de uso de informações, prestação de contas dos responsáveis pelo Tratamento de Dados Pessoais e conceder direitos aos seus Titulares. Em caso de eventual descumprimento da LGPD, a Empresa poderá ficar sujeita a sanções administrativas que incluem, por exemplo, a imposição de multas, além de eventuais condenações na esfera judicial.

Ressalta-se, ainda, que um descumprimento da LGPD poderá representar danos de imagem à Empresa perante Terceiros, que poderão incluir:

- danos à reputação e perda da confiança dos investidores
- publicidade negativa
- perda de negócios
- interrupção operacional
- sanções e litígios

3. Para que serve o Programa?

Um programa de privacidade e proteção de Dados Pessoais bem construído e abrangente é uma ferramenta eficaz de gerenciamento de riscos. A LGPD exige que todos os Empregados estejam cientes de seu conteúdo e cumpram os seus requisitos. É importante que os Dados Pessoais sejam objeto de Tratamento de maneira consistente com a LGPD e este Programa.

3.1. Vinculação ao Programa da Brookfield Asset Management Inc.

O presente Programa está alinhado com os princípios e conceitos previstos no respectivo programa da sua controladora indireta, a Brookfield Asset Management Inc. (respectivamente, “Programa BAM” e “BAM”), sendo considerado como parte integrante e vinculado ao mesmo.

De acordo com o Programa BAM, além da LGPD, a Brookfield está sujeita também a outras leis de proteção de dados aplicáveis para cada jurisdição de atuação, de modo que eventual infração cometida por uma unidade de negócio poderá implicar eventual responsabilização da BAM e/ou dos seus respectivos gestores.

Desta forma, devemos:

- realizar avaliações de risco de privacidade e proteção de Dados Pessoais, considerando as leis aplicáveis;
- ter políticas e processos em vigor para cumprir as exigências legais aplicáveis;
- incluir privacidade e proteção de Dados Pessoais nos nossos relatórios; e
- ter um processo de resposta a incidentes.

As políticas acerca de privacidade e proteção de Dados Pessoais instituídas pela Brookfield Properties podem ser compartilhadas com as unidades de negócios, que devem avaliar quais políticas e procedimentos que melhor atendem aos seus respectivos riscos de privacidade e proteção de Dados Pessoais.

3.2. Documentos deste Programa

O 'Anexo A' inclui uma breve descrição dos documentos incluídos neste Programa. Vários documentos são internos e funcionam como um guia para a Empresa e seus Empregados.

3.3. Governança e Liderança pelo Exemplo

A administração da Brookfield Properties está comprometida com o cumprimento de todas as exigências legais e regulamentares aplicáveis, incluindo aquelas relacionadas à proteção e privacidade de Dados Pessoais, cabendo à mesma o exemplo, liderança e supervisão para o desenvolvimento, implementação e operação do Programa.

A Brookfield Properties conta com um Comitê de Privacidade e Proteção de Dados Pessoais (o "Comitê"), o qual foi constituído para zelar pelo cumprimento deste Programa, da LGPD e das exigências legais e regulamentares aplicáveis relacionadas a privacidade e proteção de Dados Pessoais.

O Encarregado é a pessoa designada que será responsável pela representação da Brookfield Properties perante o Governo e os Titulares, bem como pelo monitoramento e desenvolvimento deste Programa, reportando-se ao Comitê. As funções e responsabilidades de governança no âmbito deste Programa estão descritas no 'Anexo B'.

3.4. Monitoramento de Conformidade

O Encarregado deve avaliar a conformidade deste Programa, dos documentos a ele relacionados, bem como de todas as práticas da Brookfield Properties com a LGPD e demais legislações de proteção de Dados Pessoais aplicáveis por meio de avaliações periódicas.

3.5. Comunicação e Treinamento

O objetivo deste Programa é garantir que as políticas e procedimentos de privacidade e proteção de Dados Pessoais sejam incorporados e compreendidos por meio de comunicação interna e externa, incluindo treinamentos. A filosofia e as diretrizes deste

Programa devem ser comunicadas aos Empregados e a Terceiros com quem fazemos negócios, quando apropriado.

3.6. Contatos-Chave

Se tiver alguma dúvida relacionada a este Programa ou aos documentos aqui mencionados, entre em contato com:

Encarregado

Diogo Lenneberg

lgpd_encarregadobpg@brookfieldproperties.com

(11) 2540-9258

3.7. Mudança Regulatória

O acompanhamento de mudanças regulatórias será feito pelo Departamento Jurídico e, havendo alterações, o Encarregado comunicará às pessoas chaves conforme área de competência relacionada à um plano de ação e prazo para a implantação das atualizações, bem como avaliará a necessidade de convocar o Comitê.

4. Princípios Fundamentais

Os seguintes princípios são basilares e devem ser observados em qualquer atividade de Tratamento de Dados Pessoais realizados pela Empresa:

4.1 Finalidade: Dados Pessoais somente devem ser tratados para uma finalidade específica, um propósito que seja legítimo, explícito, delimitado e informado ao Titular, não sendo permitido o Tratamento posterior que seja incompatível com as finalidades identificadas.

4.2 Adequação: Todo Tratamento de Dados Pessoais deve ser adequado ao propósito indicado e compatível com as finalidades que foram informadas ao Titular.

4.3 Necessidade: Para que o Tratamento seja considerado lícito, deve ser utilizado o mínimo de Dados Pessoais necessários para o cumprimento de determinada finalidade. Os Dados Pessoais devem ser pertinentes, proporcionais e não excessivos em relação ao propósito do Tratamento, de modo que não devem ser coletados, processados ou armazenados mais Dados Pessoais do que o estritamente imprescindível para o propósito informado ao Titular.

4.4 Livre acesso: Titulares possuem o direito de obter acesso à integralidade de seus Dados Pessoais, bem como de consultar a Empresa sobre a forma e duração do Tratamento de seus Dados Pessoais, ou de confirmar se os seus Dados Pessoais são tratados pela Empresa. A resposta a esses questionamentos deve ser realizada de forma facilitada e gratuita, não podendo ser cobrada qualquer taxa do titular ou criado qualquer empecilho que dificulte o exercício dos seus direitos de livre acesso.

4.5 Qualidade dos dados: Os Dados Pessoais tratados pela Empresa devem ser claros, exatos, relevantes e atualizados, de acordo com a sua necessidade e com os propósitos do Tratamento. Não devem ser tratados Dados Pessoais desatualizados ou irrelevantes para a finalidade indicada.

4.6 **Transparência:** A Empresa deve fornecer informações claras, precisas e facilmente acessíveis para os Titulares sobre as suas operações de Tratamento de Dados Pessoais, inclusive sobre a identidade dos agentes de Tratamento.

4.7 **Segurança de Dados:** A Empresa deve utilizar medidas de segurança técnicas, administrativas e organizacionais adequadas para garantir que os Dados Pessoais tratados estejam protegidos, impedindo acessos não autorizados ou situações acidentais ou ilícitas de destruição, adulteração, perda, comunicação, compartilhamento ou difusão de Dados Pessoais, inclusive nos casos em que o Tratamento for realizado por terceiros em nome da Empresa.

4.8 **Prevenção:** A Empresa deve adotar medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais.

4.9 **Não discriminação:** Os Dados Pessoais não devem ser tratados para qualquer propósito discriminatório ilícito ou abusivo.

4.10 **Responsabilização e prestação de contas:** É obrigação da Empresa estabelecer medidas internas para comprovar que está cumprindo com as regras previstas nas legislações de proteção de Dados Pessoais, especialmente a LGPD, e que essas medidas são eficazes para a observância das normas.

5. **Privacy by Design**

O conceito de *privacy by design*, ou proteção de dados desde a concepção, se refere à metodologia que considera questões de privacidade e proteção de Dados Pessoais na fase de elaboração de qualquer novo sistema, serviço, produto ou processo e, posteriormente, durante todo o ciclo de vida do respectivo projeto.

A privacidade deve ser o ponto de partida para o desenvolvimento de qualquer novo projeto, de modo que venha a incorporar a estrutura técnica dos produtos e serviços oferecidos pela Empresa. Para tanto, é necessário que sejam elaboradas medidas técnicas e organizacionais aptas para implementar os princípios dispostos na LGPD.

Seguir o conceito de *privacy by design* significa se antecipar aos problemas e incidentes, avaliando quais consequências poderiam surgir em relação à privacidade no desenvolvimento de qualquer produto, serviço, processo ou projeto, e, desde o início, preocupar-se em como resolver essa situação de imediato, antes mesmo que uma ação corretiva seja necessária.

A Empresa deverá garantir que sejam adotadas as devidas medidas técnicas e organizacionais para que todos os princípios do *privacy by design* sejam seguidos cotidianamente, de acordo com os passos indicados abaixo:

- 1º Passo - Identificação de Finalidade: Identificar a finalidade de determinado projeto é de extrema importância para garantir que você tenha uma clara visão sobre os propósitos específicos dos Tratamentos de Dados Pessoais que serão necessários para sua consecução do projeto e para assegurar que eles sejam adequados e proporcionais àquela finalidade.
- 2º Passo – Coleta de Dados e Uso: Identificar quais Dados Pessoais serão essenciais para o projeto, lembrando que o Tratamento deve ser realizado sobre o mínimo necessário para se alcançar as finalidades determinadas na etapa acima. Isso quer dizer que se o projeto pode ser implementado sem que

sejam conhecidos dados como o nome do Titular, seu e-mail, endereço, telefone, e outros dados de contato, essas informações não devem ser coletadas. Se o projeto envolver o tratamento de Dados Pessoais Sensíveis, as considerações com privacidade devem ser ainda mais acentuadas, uma vez que os riscos são maiores.

- 3º Passo – Qualidade dos Dados: Os Dados Pessoais devem ser completos, atualizados, corretos, evitando-se que o projeto envolva o Tratamento de dados antigos, desatualizados ou equivocados.
- 4º Passo – Gestão de Acessos: É necessário ter clareza a respeito de quem precisará ter acesso aos Dados Pessoais no desenvolvimento do projeto, limitando o número de colaboradores com acesso para evitar riscos maiores de incidentes de segurança. Somente Empregados que realmente precisem conhecer as informações para o desenvolvimento do projeto devem conseguir visualizar os Dados Pessoais. Acrescentar camadas de privilégios é uma boa prática, no sentido de minimizar ainda mais os Empregados com acesso a determinadas informações.
- 5º Passo – Retenção e Exclusão: Considerando que a privacidade e proteção de dados devem ser garantidas em todo o ciclo de vida dos dados, desde a sua coleta até sua exclusão, é primordial avaliar se o projeto em desenvolvimento demandará a retenção de Dados Pessoais e por quanto tempo. Se o projeto puder ser implementado sem que os Dados Pessoais sejam armazenados posteriormente, eles devem ser excluídos imediatamente após o seu uso. Caso seja necessário armazenar os Dados Pessoais, os períodos de retenção já devem ser estabelecidos desde o início, e medidas devem ser implementadas para garantir que após o decurso de referido período os dados sejam definitivamente excluídos, de modo seguro. Se possível, mecanismos de exclusão automática dos dados após o decurso do prazo de retenção devem ser considerados. Nos casos de necessidade de retenção dos dados para o desenvolvimento do projeto, deve ser avaliada a possibilidade de se anonimizar os Dados Pessoais, permitindo o seu uso sem trazer maiores riscos à Empresa, uma vez que dados anonimizados estão fora do escopo da LGPD.
- 6º Passo – Segurança: Avaliar a segurança que será garantida aos Dados Pessoais durante todo o ciclo de vida do projeto também é de extrema importância. Técnicas para proteger os dados contra perda, adulteração, acesso ou uso indevido, e tornar os dados ininteligíveis, devem ser consideradas quando do desenvolvimento de qualquer projeto novo.

6. Controle e Histórico de Versões

Data	Versão	Sumário
14/03/2024	01/2024	Criação do instrumento normativo
28/02/2025	02/2025	Revisão do instrumento normativo

7. Aprovações

Descrição	Versão	Vigência
Programa de Privacidade	1/2025	28/02/2025 a 28/02/2027

Emissor(es): Diogo Lenneberg

Revisor: Anderson Zaidan e Bianca Siqueira

Aprovador(es): Roberto Perroni (aprovado eletronicamente)

Anexo A

1. Glossário

Sem prejuízo das definições atribuídas no âmbito da LGPD, para os fins deste Programa, os termos abaixo definidos terão os seguintes significados:

- a) **Controlador** – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.
- b) **Dado(s) Pessoal(is)** – informação relacionada a pessoa natural identificada ou identificável, como, por exemplo, um nome, um número de identificação e localização.
- c) **Dado(s) Pessoal(is) Sensível(is)** – São Dados Pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados relativos à vida sexual ou orientação sexual do Titular.
- d) **Empregado** – refere-se a todo e qualquer conselheiro, administrador, diretor e demais funcionários da Empresa.
- e) **Encarregado** – pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os Titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).
- f) **Governo** – qualquer entidade integrante da administração pública direta ou indireta, incluindo a União, os Estados, os Municípios e o Distrito Federal, bem como seus órgãos, ministérios, secretarias, departamentos, subsecretarias, autarquias, empresas, instituições, agências e órgãos de propriedade ou controlados pelo governo e outras entidades públicas.
- g) **Operador** – pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador.
- h) **Terceiro** – refere-se a todo e qualquer prestador de serviços, fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, locatário, cessionário de espaço comercial, seja pessoa física ou jurídica, independentemente de contrato formal ou não, que utiliza o nome da Empresa para qualquer fim ou que presta serviços, fornece materiais, interage com o Governo ou com outros em nome da Empresa.
- i) **Titular** – pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.
- j) **Tratamento** – toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Anexo B

Documentos do Programa de Privacidade e Proteção de Dados Pessoais

1. Registro de Tratamento de Dados Pessoais (“RoP” ou “ROPA”)

O RoP é o documento no qual todos os processos da Empresa que envolvam fluxo de Tratamento de Dados Pessoais são mapeados, conforme disposto na LGPD.

2. Regimento do Comitê de Privacidade (“Regimento”)

Documento que estabelece as finalidades, abrangência, atribuições, subordinação, composição, funcionamento e responsabilidades do Comitê de Privacidade da Empresa.

3. Política de Privacidade e Proteção de Dados Pessoais (“Política”)

A Política é o documento interno que descreve a forma pela qual os Dados Pessoais devem ser tratados pelos Empregados para cumprir as normas de proteção de dados e garantir a conformidade com a lei aplicável, incluindo a LGPD e este Programa.

4. Terceiros

4.1 Cláusula de Proteção de Dados Pessoais

Quando um Terceiro (por exemplo, um fornecedor de TI) processa, retém, acessa ou usa Dados Pessoais para ou em nome da Empresa (e não processa os Dados Pessoais para seus próprios fins), a LGPD exige que um contrato por escrito seja firmado e que esse contrato contenha cláusulas específicas para proteção e privacidade de Dados Pessoais. Essas cláusulas são estabelecidas para garantir que o processamento realizado por Terceiros cumpra todas as exigências legais aplicáveis.

4.2 Lista de Verificação de Diligência em Privacidade e Proteção de Dados Pessoais

A lista de verificação estabelece as questões relevantes que devem ser consideradas ao realizar a diligência em relação a aquisições, empreendimentos conjuntos (*joint ventures*) ou demais transações corporativas. Tal lista de verificação não pretende ser exaustiva e a diligência necessária dependerá das especificidades de cada transação.

4.3 Cláusulas de Confidencialidade (quando a Empresa for o divulgador de Dados Pessoais)

Quando a Empresa divulgar Dados Pessoais (por exemplo, passaportes de diretores/informações sobre empregados) a Terceiros, deverão ser incluídas disposições contratuais específicas para assegurar que o Terceiro receptor dos Dados Pessoais seja contratualmente obrigado a cumprir a lei aplicável, incluindo a LGPD. Observe que, se o Terceiro for um fornecedor que processará apenas os Dados Pessoais em nome da Empresa, prevalecerá o disposto no ‘item 4a’ acima.

4.4 Cláusulas de Confidencialidade (quando a Brookfield for a receptora de Dados Pessoais)

Quando a Empresa obtiver Dados Pessoais (por exemplo, passaportes de diretores/informações sobre colaboradores) de Terceiros, esses Terceiros podem exigir que os termos de privacidade sejam incluídos no acordo de confidencialidade ou outros documentos aplicáveis.

4.5 Norma de Avaliação de Riscos de Terceiros

O documento estabelece diretrizes, responsabilidades e procedimentos que permitam à Empresa conhecer e avaliar seus Terceiros e, conseqüentemente, auxiliar no gerenciamento de eventuais riscos de imagem, suborno, corrupção e lavagem de dinheiro, privacidade e proteção de dados, entre outros, decorrentes da relação com seus Terceiros.

5. Política de Segurança da Informação

A Política de Segurança da Informação descreve o processo de proteção da confidencialidade, disponibilidade e integridade das informações. Referida política foi estabelecida para proteger todos os ativos que contêm informações, incluindo, entre outros, documentos, computadores, dispositivos móveis e componentes de infraestrutura de rede pertencentes, alugados ou mantidos, controlados e/ou usados pela Brookfield Properties.

6. Plano de Resposta a Incidentes de Segurança da Informação

O Plano de Resposta a Incidentes de Segurança da Informação define a estrutura e os processos desenvolvidos para (i) detectar e reagir a incidentes de segurança da informação, (ii) determinar seu escopo, riscos e a resposta apropriada, (iii) comunicar os resultados e riscos a todas as partes interessadas relevantes e (iv) reduzir a probabilidade de recorrência. Referido plano deve ser lido em conjunto com outras políticas e procedimentos da Brookfield Properties, incluindo a Política de Segurança da Informação (consulte o 'item 5' acima) e a Política de Privacidade de Proteção de Dados Pessoais (consulte o 'item 3' acima).

8. Contrato de Transferência Internacional de Dados

O Contrato de Transferência Internacional de Dados visa garantir a conformidade com as leis de proteção de dados aplicáveis de todas as jurisdições envolvidas em eventual transferência internacional. As entidades que detêm dados de investidores precisarão implementar esse contrato. Quaisquer unidades de negócios que transfiram Dados Pessoais em nome da Empresa devem firmar um acordo semelhante com os respectivos destinatários dos Dados Pessoais.

9. Aviso sobre Privacidade e Proteção de Dados de Empregados

O Aviso sobre Privacidade e Proteção de Dados de Empregados resume as maneiras pelas quais a Brookfield Properties coleta, usa, divulga e gerencia Dados Pessoais de seus Empregados e respectivos dependentes (conforme aplicável), além de especificar os direitos dos mesmos em relação aos seus Dados Pessoais. Tal aviso deve ser fornecido ao Empregado na sua admissão e ajustado sempre que necessário.

10. Aviso sobre Privacidade e Proteção de Dados de Candidatos

O Aviso sobre Privacidade e Proteção de Dados de Candidatos resume as maneiras pelas quais a Brookfield Properties coleta, usa, divulga e gerencia Dados Pessoais de indivíduos que se candidatam a emprego na Brookfield Properties, além de especificar os direitos dos Titulares em relação a seus Dados Pessoais. Tal aviso deve ser fornecido ao candidato quando seus Dados Pessoais forem coletados.

11. Aviso de Privacidade

O Aviso sobre Privacidade resume as maneiras pelas quais a Brookfield Properties coleta, usa, divulga e gerencia todas as categorias de Dados Pessoais, bem como suas respectivas finalidades. Além disso, o documento aponta quais são as bases legais utilizadas para o Tratamento de dados, bem como informações a respeito do compartilhamento, armazenamento, retenção e transferência internacional de dados. Adicionalmente, dá transparência acerca das medidas de segurança utilizadas pela Empresa, dos direitos dos Titulares previstos na LGPD e de como exercê-los.

12. Políticas e Avisos do Website da Brookfield no Brasil

12.1 Política de Proteção de Dados e Aviso de Privacidade do Website da Brookfield no Brasil

A Política do Website da Brookfield no Brasil sobre Privacidade e Proteção de Dados descreve as maneiras pelas quais a Brookfield Properties coleta, usa, divulga e gerencia Dados Pessoais de usuários do site da Brookfield Properties, além de especificar os direitos dos Titulares em relação a seus Dados Pessoais.

12.2 Termos de Uso do Site

Os Termos de Uso do site são os termos que governam o uso do site da Brookfield Properties pelos usuários.

12.3 Política de Cookies

A Política de Cookies informa aos usuários do site da Brookfield no Brasil como são utilizados cookies e como os usuários podem bloquear os cookies. Cookies são pequenos arquivos de texto que armazenam informações sobre a interação do usuário com um site temporariamente ou permanentemente no disco rígido do dispositivo do usuário.

13. Política de Retenção de Dados Pessoais

A Política é o documento interno que determina o período necessário para o armazenamento de Dados Pessoais, de acordo com a legislação aplicável e garantindo a proteção legal da Empresa.

14. Procedimento para Uso do Consentimento

Guia contendo regras e identificando desafios práticos que tenham relação com o consentimento, quando este tiver sido a base legal eleita para fundamentar o Tratamento de Dados Pessoais.

Além disso, este documento fornece exemplos de como se pode obter um consentimento válido de acordo com a LGPD.

15. Manual de Atendimento aos Titulares de Dados

Documento que esclarece como responder e quais as boas práticas de contato com o Titular de dados no exercício de seus direitos, direcionando os Empregados e Terceiros que tenham contato com o Titular de dados no exercício de seus direitos junto à Empresa.

16. Orientações para a estruturação do cargo de DPO

O documento traz diretrizes básicas para que o Encarregado (DPO) seja de fato o centro focal no que tange a proteção de Dados Pessoais dentro da Empresa, responsável por auxiliar a organização na adequação à LGPD e na contínua governança de privacidade proteção de Dados Pessoais.

17. Modelo de Teste de Legítimo Interesse

O modelo de Teste de Legítimo Interesse deverá ser aplicado sempre que determinado processo de Tratamento de Dados Pessoais tiver como base legal o interesse legítimo, nos termos do artigo 10 da LGPD.

18. Modelo de Relatório de Impacto

O modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deverá ser aplicado sempre que uma operação envolvendo o Tratamento de Dados Pessoais puder ocasionar riscos elevados aos Titulares, nos termos do artigo 38 da LGPD.

19. Modelo de Comunicação de Incidentes à Autoridade Nacional de Proteção de Dados

Modelo disponibilizado pela Autoridade Nacional de Proteção de Dados, em seu portal eletrônico, para a comunicação de eventuais incidentes de segurança e incidentes de privacidade.

Anexo C
Papéis e Responsabilidades

I. Brookfield Properties

A Brookfield Properties nomeou o Encarregado de Privacidade conforme abaixo.

Em caso de dúvida ou preocupação sobre o tratamento de dados pessoais ou sobre esta Política, entre em contato com a pessoa relevante para a respectiva jurisdição ou região usando as informações de contato definidas abaixo.

Jurisdição/Região	Informações de Contato
Brasil	Diogo Lenneberg (Brookfield Properties Legal Counsel)

II. Comitê da Brookfield Properties

O Comitê da Brookfield Properties é responsável pelo:

- a. cumprimento das obrigações aplicáveis sobre Privacidade e Proteção de Dados, incluindo a LGPD; e
- b. eleger e destituir o Encarregado.

O Encarregado da Brookfield Properties é responsável por:

- a. monitorar a conformidade deste Programa;
- b. revisar e aprovar periodicamente os procedimentos de proteção de dados e políticas relacionadas;
- c. lidar com as consultas de proteção de dados de Empregados;
- d. lidar com as solicitações de dados feitas por Titulares;
- e. monitorar o cumprimento das exigências constantes da seção 'Vinculação ao Programa da Brookfield Asset Management Inc.' deste Programa;
- f. organizar treinamento e consultoria em proteção de dados para Empregados; e
- g. manter o Comitê informado acerca de alterações nas atividades de Tratamento de dados.

O Departamento Jurídico é responsável por:

- a. revisar e aprovar contratos ou acordos com Terceiros, incluindo a celebração de acordos de proteção de Dados Pessoais e eventuais termos de Transferência.
- b. dar seguimento ao processo de avaliação de riscos de privacidade no que tange a contratação de Terceiros.
- c. manter o Comitê informado sobre eventuais exigências legais de proteção de dados, privacidade e segurança cibernética, incluindo suas atualizações
- d. revisar o ROPA (Registro de Operações de Tratamento de Dados Pessoais) a cada 2 anos ou na medida em que a legislação defina.

O Departamento de TI é responsável por:

- a. assegurar que os sistemas, serviços e equipamentos usados para armazenar Dados Pessoais cumpram as normas de segurança aceitáveis;

- b. executar verificações regulares para assegurar que o hardware e o software funcionem corretamente; e
- c. avaliar os serviços de Terceiros que a Brookfield Properties esteja considerando usar para armazenar ou processar Dados Pessoais.

Cada Empregado é responsável por conduzir suas atividades em observância com a legislação aplicável, incluindo a LGPD, bem como por cuidar dos Dados Pessoais que estejam sob seu Tratamento.