



Programa de Privacidade e Proteção de Dados Pessoais da Brookfield Brasil Ltda.

Janeiro de 2021

Sumário

I. Introdução.....	3
II. Glossário.....	3
III. Por que a Privacidade e Proteção de Dados Pessoais são tão importantes?	4
IV. Para que serve o Programa?	5
a. Vinculação ao Programa da Brookfield Asset Management Inc.....	5
b. Documentos deste Programa	5
c. Governança e Liderança pelo Exemplo.....	5
d. Monitoramento de Conformidade	6
e. Comunicação e Treinamento.....	6
f. Contatos-Chave.....	6
Anexo A.....	7
Anexo B.....	10

I. Introdução

A Brookfield no Brasil (“**Brookfield**”) 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 Brasil Ltda. (respectivamente, “**Programa**” e “**BRB**”) 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 BRB, sua controladora e suas empresas controladas ou sob sua administração, ressalvadas as entidades Brookfield que tenham programas, políticas e práticas próprias acerca de privacidade e proteção de dados pessoais, incluindo, sem limitação, as empresas abaixo (cada uma delas doravante designada simplesmente “**Empresa**”):

- a) Brookfield Brasil Asset Management Investimentos Ltda.
- b) Brascan Projetos de Recuperação Ambiental Ltda.
- c) Brascan Natural Resources Ltda.
- d) Brookfield Corretora de Seguros Ltda.
- e) BRKB Distribuidora de Títulos e Valores Mobiliários S.A.

II. Glossário

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

- a) **Dado(s) Pessoal(is)** – informação relacionada a pessoa natural identificada ou identificável, como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.
- b) **Empregado** – refere-se a todo e qualquer conselheiro, administrador, diretor e demais funcionários da Empresa.
- c) **Encarregado** – pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados (ANPD).

- d) **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.
- e) **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.
- f) **Titular** – pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.
- g) **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.

III. 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 Dados Pessoais, responsabilização dos agentes responsáveis pelo Tratamento de Dados Pessoais e a garantia de direitos aos Titulares. Em caso de eventual descumprimento da LGPD, a Brookfield poderá ficar sujeita a ações judiciais e sanções administrativas que incluem, por exemplo, a imposição de multas.

Além disso, um descumprimento da LGPD poderá representar danos de imagem à Brookfield perante Terceiros, que poderão incluir:

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

IV. 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 e cumpram os seus requisitos. É importante que os Dados Pessoais sejam objeto de Tratamento de maneira consistente com a LGPD e este Programa.

a. 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 referido programa.

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 em eventual responsabilização da empresa controladora e/ou dos seus respectivos gestores.

Desta forma, devemos:

1. realizar avaliações de risco de privacidade e proteção de dados pessoais, considerando as leis aplicáveis;
2. ter políticas e processos em vigor para cumprir as exigências legais aplicáveis;
3. incluir privacidade e proteção de dados pessoais nos nossos relatórios; e
4. ter um processo de resposta a incidentes.

As políticas acerca de privacidade e proteção de dados instituídas pela BRB 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.

b. 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 Brookfield e seus Empregados.

c. Governança e Liderança pelo Exemplo

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

A Empresa 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 Empresa perante o Governo, 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’.

d. Monitoramento de Conformidade

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

e. 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.

f. Contatos-Chave

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

Encarregado

Felipe Carneiro

Encarregado-LGPD@brookfield.com

(21) 3725-7621

* * *

Anexo A

Documentos do Programa de Privacidade e Proteção de Dados Pessoais

1. 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.

2. Terceiros

a. Cláusula de Proteção de Dados Pessoais

Quando um Terceiro (por exemplo, um fornecedor de TI) trata, retém, acessa ou usa Dados Pessoais para ou em nome da Brookfield (e não trata os Dados Pessoais para seus próprios fins), é recomendável 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 tratamento realizado por Terceiros cumpra todas as exigências legais aplicáveis.

b. 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.

c. Cláusulas de Confidencialidade (quando a Brookfield for o divulgador de Dados Pessoais)

Quando a Brookfield revelar 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 tratará apenas os Dados Pessoais em nome da Brookfield, prevalecerá o disposto no ‘item 2a’ acima.

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

Quando à Brookfield forem revelados 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.

3. 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 contém informações, incluindo, entre outros, documentos, computadores, dispositivos móveis e componentes de infraestrutura de rede pertencentes, alugados ou mantidos, controlados e/ou usados pela Empresa, conforme aplicável.

4. 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 as outras políticas e procedimentos, incluindo a Política de Segurança da Informação (consulte o 'item 3' acima) e a Política de Privacidade e Proteção de Dados Pessoais (consulte o 'item 1' acima).

5. 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 desejarem transferir dados ao exterior precisarão implementar esse contrato. Quaisquer unidades de negócios que transfiram Dados Pessoais em nome da Brookfield devem firmar um acordo semelhante com os respectivos destinatários dos Dados Pessoais.

6. 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 coleta, usa, divulga e gerencia Dados Pessoais de seus Empregados e respectivos dependentes (conforme aplicável), além de especificar os seus direitos em relação aos seus Dados Pessoais. Tal aviso deve ser fornecido ao Empregado na sua admissão e ajustado sempre que necessário.

7. 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 Empresa coleta, usa, divulga e gerencia Dados Pessoais de indivíduos que se candidatam a emprego na Empresa, 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.

8. Políticas e Avisos do Website

a. Política de Proteção de Dados e Aviso de Privacidade do Website

A Política de Proteção de Dados e Aviso de Privacidade do Website descreve as maneiras pelas quais a Empresa coleta, usa, divulga e gerencia Dados Pessoais de usuários do site da Empresa, além de especificar os direitos dos Titulares em relação a seus Dados Pessoais.

b. Termos de Uso do Site

Os Termos de Uso do Site são os termos que regem o uso do site da Empresa pelos usuários.

c. Política de Cookies

A Política de Cookies informa aos usuários do site da Empresa 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.

Anexo B
Papéis e Responsabilidades

I. BAM

O Conselho de Administração da BAM é responsável por garantir que a BAM cumpra suas obrigações legais. A BAM nomeou Encarregados de Privacidade em cada jurisdição ou região conforme a tabela 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 de Consultores Regulatórios e Diretores de Privacidade
Ásia	Aanandjit Sunderaj (Singapore Regulatory Counsel); Al-Ammin Ali Zahabar (Director, Legal & Regulatory); Jolyn Ho (Director, Legal & Regulatory)
Austrália	Michael Ryan (Australian Regulatory Counsel)
Brasil	Felipe Carneiro (Director, Technology Services)
Canadá	Kathy Sarpash (Canada Regulatory Counsel)
EMEA	Philippa Elder (Regulatory Counsel)
Índia	Swati Mandava
EUA	Ronald Fisher-Dayn (Corporate Compliance); Renee Mallen (US Privacy Counsel)

II. Comitê da Empresa

O Comitê da Empresa é responsável pelo:

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

Além de outras atribuições previstas na LGPD, o Encarregado da Empresa 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 relacionadas a Dados Pessoais 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. manter o Comitê informado sobre eventuais exigências legais de proteção de dados, privacidade e segurança cibernética, incluindo suas atualizações.

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 Empresa 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.