POLÍTICA DE GOVERNANÇA DE PROTEÇÃO DE DADOS PESSOAIS

SUMÁRIO

1 OBJETIVO 3

2 ABRANGÊNCIA 3

3 REFERÊNCIAS 3

4 CONCEITOS 4

5 PRINCÍPIOS NORTEADORES 7

6 RESPONSABILIDADES 9

7 INFORMAÇÕES DE CONTROLE 10

1 OBJETIVO

A B3 S.A. – Brasil, Bolsa, Balcão ("B3"), está comprometida em manter sempre as melhores práticas de mercado no que diz respeito a questões de Proteção de Dados Pessoais que são tratados em seus ambientes.

Esta Política tem por objetivo apresentar os princípios e as diretrizes que norteiam as atividades de Tratamento de Dados Pessoais realizadas pela B3.

Aplicam-se também as disposições específicas constantes no item 5.2 desta Política para os casos a seguir, denominados de "Tratamentos GDPR", caso:

(i) o Tratamento seja realizado no contexto das atividades desenvolvidas em estabelecimentos da B3 na União Europeia; ou,

(ii) o Tratamento de Dados Pessoais incidir sobre Titulares localizados na União Europeia (a) no âmbito da oferta de bens ou serviços a esses Titulares ou (b) quando pretenda monitorar o seu perfil comportamental e o comportamento submetido ao mencionado monitoramento ocorra na União Europeia[1].

2 ABRANGÊNCIA

Esta Política se aplica a administradores, funcionários, estagiários, aprendizes, fornecedores, prestadores de serviços e parceiros da B3 S.A. – Brasil, Bolsa, Balcão, suas controladas no exterior, bem como à BSM Supervisão de Mercados (BSM), à Cetip Info Tecnologia S.A., ao B3 Social e demais associações, mantenedora, honorária ou fundadora (Companhia).

3 REFERÊNCIAS

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados ("LGPD");

[1] Para consultar uma lista permanentemente atualizada dos países que pertencem à União Europeia, acesse esta página: https://europa.eu/european-union/about-eu/countries_pt.

- Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril ("GDPR"); e

- Política de Segurança da Informação.

4 CONCEITOS

- **"Dado(s) Pessoal(ais)"** significa qualquer informação que, direta ou indiretamente, sozinha ou acompanhada de outros dados, identifique ou possa identificar uma pessoa física. São exemplos de dados pessoais: nome, CPF, número de Protocolo de Internet (IP), endereço de e-mail, número de conta bancária, perfil financeiro, identificação de contribuinte, registro profissional, geolocalização, dentre outros. Incluem-se neste conceito os Dados Pessoais Sensíveis, conforme definição abaixo;

- **"Dado(s) Pessoal(ais) Sensível(is)"** significa um dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

  - Quando houver Tratamento GDPR: significa qualquer Dado Pessoal que revele a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

- **"Dado(s) Anonimizado(s)"** significa o dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

  - Quando houver Tratamento GDPR: significa o dado relativo a um titular que não pode ser identificado após a aplicação de técnicas de anonimização. A anonimização é uma técnica que resulta do

Tratamento de Dados Pessoais a fim de lhes retirar elementos suficientes para que deixe de ser possível identificar o Titular, de forma irreversível;

- **"Dado Pessoal Pseudoanonimizado"** significa um tipo de Dado Pessoal tratado de forma a não ser mais relacionável a uma pessoa específica sem que seja necessário recorrer a informações suplementares, desde que tais informações sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais que assegurem que os Dados Pessoais não possam ser atribuídos a uma pessoa identificada ou identificável;

- **"Titular(es)"** significa qualquer pessoa física identificada ou que possa ser identificada pelo Tratamento dos Dados Pessoais ou Dados Pessoais Sensíveis;

- **"Tratamento"** significa toda e qualquer operação realizada com os Dados Pessoais ou Dados Pessoais Sensíveis, incluindo, mas não se limitando, à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

- **"Violação de Dados Pessoais"** significa toda e qualquer situação, acidental ou intencional, praticada mediante culpa ou dolo, que provoque, em relação a Dados Pessoais: (i) a destruição; (ii) a perda; (iii) a alteração; (iv) a comunicação, difusão ou divulgação; ou (v) o acesso não autorizado;

- **"Controladora" ou "*Controller*" ou "Responsável pelo Tratamento"** significa a Parte a quem compete as decisões relativas ao Tratamento de Dados Pessoais;

- **“Operadora” ou “*Processor*” ou “Subcontratante”** significa a Parte que realiza o Tratamento de Dados Pessoais em nome e sob as instruções da Controladora;

- **“Controladora(s) conjunta(s)”** significa quando as Partes em conjunto têm a competência de decidir sobre o Tratamento de Dados Pessoais;

- **“Relatório de Impacto à Proteção de Dados Pessoais” (RIPD) ou “*Data Protection Impact Assessment*” (“DPIA”)** significa a documentação da Controladora que contém a descrição e avaliação dos processos de Tratamento de Dados Pessoais, seus eventuais riscos e impactos às liberdades civis e aos direitos fundamentais dos Titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

- **“Encarregado” ou “*Data Protection Officer*” (“DPO”)** significa pessoa indicada pela B3 para atuar como canal de comunicação entre a Companhia, os Titulares dos Dados Pessoais, a Autoridade Nacional de Proteção de Dados (“ANPD”) e a autoridade pública independente criada por um Estado-Membro da União Europeia com a responsabilidade pela fiscalização da aplicação do GDPR, bem como as demais responsabilidades estabelecidas no item 6.1;

- **“Ciclo de vida do Dado Pessoal”** representa todos os fluxos de Tratamento aos quais o Dado Pessoal é submetido durante sua existência nos sistemas da B3;

- **“Transferência Internacional de Dados Pessoais”** significa a transferência de dados pessoais para país estrangeiro ou organismo internacional;

- **“Transferência Internacional de Dados Pessoais para fins de GDPR”** significa a transferência de Dados Pessoais de um país da União Europeia para um país terceiro (não localizado na União Europeia) ou uma organização internacional, podendo a transferência ocorrer entre dois ou mais Responsáveis pelo Tratamento, Responsáveis pelo

Tratamento e Subcontratantes ou simplesmente ser alojados num espaço virtual fora da União Europeia sem que os Dados Pessoais sejam transferidos para outra pessoa física ou jurídica;

- **"Terceiro"** significa pessoa física ou jurídica, autoridade pública, serviço ou organismo que seja Prestador de Serviço, Parceiro, Cliente, Fornecedor ou qualquer outro terceiro;

- **"Autoridade Competente"** significa a Autoridade Nacional de Proteção de Dados ("ANPD") e a autoridade pública independente criada por um Estado-Membro da União Europeia com a responsabilidade pela fiscalização da aplicação do GDPR;

- **"Representante"** significa uma pessoa física ou jurídica estabelecida na União Europeia que, designada por escrito pelo Responsável pelo Tratamento ou Subcontratante que tenha o seu estabelecimento fora da União Europeia, representa o Responsável pelo Tratamento ou o Subcontratante no que se refere às suas obrigações respetivas nos termos do GDPR.

5 PRINCÍPIOS NORTEADORES

A B3, ao realizar qualquer atividade de Tratamento de Dados Pessoais, deve observar os seguintes princípios:

- Finalidade, licitude e lealdade;

- Adequação e limitação das finalidades;

- Necessidade;

- Livre acesso;

- Transparência;

- Segurança, Prevenção, Integridade e Confidencialidade;

- Não discriminação;
- Prestação de Contas, Responsabilidade (*accountabilty)*;
- Exatidão; e
- Limitação da conservação.

5.1 DIRETRIZES

Deve ser mantido controle direto dos Dados Pessoais que são tratados no escopo dos produtos e serviços da Companhia. Os processos de negócio, sistemas de suporte e relacionamento devem ser desenvolvidos com o mais elevado grau de segurança dos Dados Pessoais e aderência à legislação e normativos que regem o tema.

Os fluxos de Tratamento de Dados Pessoais realizados pela B3 devem ser devidamente mapeados e enquadrados em uma das bases legais previstas na legislação aplicável, mantendo o registro de atividades de Tratamento de Dados Pessoais completo.

Ademais, a Companhia deve observar as seguintes diretrizes, para garantia da governança de proteção de Dados Pessoais:

- Gestão de Terceiros: procedimentos e regras contratuais em relação aos Terceiros envolvidos nas suas atividades de Tratamento de Dados Pessoais, de modo que estes fiquem obrigados a adotar medidas técnicas e organizacionais com vistas à Proteção dos Dados Pessoais nos termos desta Política e demais leis aplicáveis.
- Relatórios de Impacto a Proteção de Dados Pessoais (“RIPD”) ou *Data Protection Impact Assessments (“DPIA”)*: elaboração e registro de DPIAs dos Tratamentos de Dados Pessoais quando assim for necessário para atender à legislação aplicável ou à solicitação de Autoridade Competente, procurando identificar as medidas necessárias para eliminar ou mitigar os altos riscos aos direitos dos Titulares.

- Direitos dos Titulares: exercício, pelos Titulares ou por representante legal, mediante uso dos canais disponíveis elencados no site principal da B3, conforme suas políticas e normativos internos.

- Transferências Internacionais: realizadas de acordo com as hipóteses autorizativas previstas na legislação aplicável.

- Privacidade e Segurança por Design e por Padrão ou *Privacy and Security by Design and by Default*: os serviços e produtos devem, desde sua concepção, ter como padrão a observância dos princípios gerais de proteção de Dados Pessoais e privacidade, bem como medidas de segurança da informação.

- Gestão de Incidentes de Violação de Dados Pessoais: estabelecimento de um Plano de Incidentes de Violação de Dados Pessoais para adoção das providências adequadas conforme a legislação aplicável.

5.2 DIRETRIZES ESPECÍFICAS PARA OS TRATAMENTOS GDPR

Na observância das Diretrizes e dos Princípios Norteadores estabelecidos nesta Política, devem ser considerados também os conceitos definidos no item 4 desta Política, indicados de forma específica.

Ademais, a B3 mantém um Representante cujos dados de contato estão disponíveis no site principal da Companhia.

6 RESPONSABILIDADES

6.1 ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS

- Gerir os processos e os procedimentos de proteção de Dados Pessoais;

- Atuar como ponto focal da Companhia em assuntos relacionados à Proteção de Dados Pessoais;

- Receber e realizar comunicações de qualquer autoridade fiscalizadora nacional ou internacional, incluindo, mas não se limitando, à ANPD, às

autoridades nacionais de proteção de dados da União Europeia, dentre outras;

- Assessorar o Representante da B3 na União Europeia nas respostas de quaisquer solicitações por ele recebidas;
- Garantir a observância aos direitos dos Titulares de Dados Pessoais; e
- Promover a conscientização e educação sobre Proteção de Dados Pessoais.

6.2 ÁREA DE PROTEÇÃO DE DADOS

- Apoiar o Encarregado na execução de suas responsabilidades.

6.3 PROPRIETÁRIOS DA INFORMAÇÃO

- Os Proprietários de Informações, que tratem Dados Pessoais e/ou Dados Pessoais Sensíveis, deverão levar em consideração as diretrizes desta Política e da Norma de Proteção de Dados Pessoais, nas atividades de classificação, proteção, controle e autorização de acesso à Informação.

7 INFORMAÇÕES DE CONTROLE

Vigência: a partir de 16 de dezembro de 2024

1ª versão: 17/08/2020.

Responsáveis pelo documento:

Responsável	Área
Elaboração	Gerência Jurídica de Produtos Não Regulados
Revisão	Gerência de Compliance Diretoria de Cyber Security Comitê de Governança e Indicação
Aprovação	Conselho de Administração

Registro de alterações:

Versão	Item Modificado	Motivo	Data
01	Versão Original	N/A	17/08/2020
02	Versão 1.0	Alteração item 7: atualização das áreas responsáveis pelo documento.	26/04/2021
03	Responsabilidades	Atualização do nome da área Diretoria de Cyber Security	28/06/2022
04	Todos os itens	Atualização da Política	11/09/2023
05	Todos os itens	Atualização da Política	16/12/2024