BRUNEL PARTNERS

POLÍTICAS & NORMAS INTERNAS

Política de Segurança da Informação (“LGPD”)

Conteúdo

1. OBJETIVO

Esta Política tem como objetivo formalizar os procedimentos e controles internos, em respeito à legislação e normas vigentes na **BRUNEL PARTNERS,** de razão social **CLIFTON CONSULTORIA DE VALORES MOBILIÁRIOS**, sociedade empresária limitada, consultoria de investimentos focada exclusivamente em investidores institucionais.

As atividades de consultoria de investimentos exigem a mais completa relação de credibilidade e confiança entre nós e nossos clientes. Exige, ademais, o compromisso inegociável com a legalidade e espírito de cooperação com os órgãos reguladores dos mercados em que atuamos.

Diante disto, esta Política de Segurança da Informação e Controles Internos ("Política") busca pela preservação da:

i. **Autenticidade** – todos os esforços serão feitos para que as informações sejam confiáveis e corretas;

ii. **Confidencialidade** – o acesso à informação é permitido somente para pessoas autorizadas e quando for de fato necessário;

iii. **Disponibilidade** – somente as pessoas autorizadas têm acesso à informação sempre que necessário; e

iv. **Integridade** – todos os esforços serão feitos para que as informações sejam exatas e completas.

O conhecimento e a adoção das medidas indicadas neste documento são de responsabilidade de todos os colaboradores da BRUNEL PARTNERS ("Brunel") e constituem fator fundamental para garantir sua conformidade com as melhores práticas de privacidade e proteção de dados pessoais.

2. ENCARREGADOS PELO TRATAMENTO DE DADOS PESSOAIS

O programa de privacidade da Brunel ("Programa") é formado por um conjunto de pessoas, processos, procedimentos e diretrizes, com o intuito de definir e cumprir estratégias e executar ações que levem a gestão adequada de controles internos de privacidade e proteção de dados pessoais pela sociedade, de forma a garantir o cumprimento de todas as leis e regulamentações aplicáveis e em vigor relacionadas a proteção de dados incluindo, sem limitação, a Lei Geral de proteção de Dados Pessoais (LGPD).

Para tanto, as estruturas, áreas e pessoas abaixo listadas estarão diretamente envolvidas na gestão do Programa e possuem as seguintes atribuições no que tange às matérias de que trata esta Política:

2.1. DATA PROTECTION OFFICER - DPO

O Data Protection Officer ("DPO") da Brunel terá as seguintes atribuições:

i. A gestão da segurança da informação na Brunel é de responsabilidade do DPO. Este é responsável pelas funções de risco, segurança e conformidade e tem o papel de manter e melhorar esta Política e seus procedimentos complementares.

ii. Organizar e/ou ministrar treinamentos em proteção de dados pessoais aos colaboradores ou prestadores de serviço, promovendo a cultura de proteção de dados pessoais na Brunel;

iii. Elaborar e/ou revisar os procedimentos internos relativos à proteção de dados pessoais;

iv. Auxiliar na definição de controles para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais e registros auditáveis de todo o ciclo de vida dos dados pessoais;

v. Apoiar na resposta aos incidentes de segurança que envolvam dados pessoais;

vi. Realizar acompanhamento legislativo/regulatório sobre o tema;

vii. Apoiar na manutenção atualizada do mapeamento dos fluxos de dados pessoais;

viii. Recomendar os requisitos adequados no caso de transferência de dados entre agentes de tratamento, especialmente transferências internacionais, além de verificar a adequação das práticas e políticas da Brunel;

ix. Responder às consultas e apresentar recomendações sobre a aplicação das regras de privacidade junto às áreas da Brunel e demais agentes de tratamento;

x. Zelar para que os titulares sejam informados sobre seus direitos, obrigações e responsabilidades sobre a proteção de dados, além de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

xi. Apoiar investigações para apuração de responsabilidade dos envolvidos em violações de dados pessoais e auxiliar na definição de aplicação das penalidades internas, quando necessário;

xii. Avaliar relatórios de impacto à proteção de dados pessoais;

xiii. Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;

xiv. Assegurar a divulgação e a disponibilidade dos documentos que compõem esta Política e outros documentos internos para proteção de dados pessoais na Brunel; e

xv. Auxiliar na aplicação das políticas internas referentes à proteção de dados pessoais.

2.2. ÁREA DE TECNOLOGIA DA INFORMAÇÃO (TI)

Compete a área de tecnologia da informação da Brunel:

i. Assegurar que todos os sistemas, serviços e equipamentos usados para o tratamento de dados pessoais estejam dentro de um padrão aceitável de segurança;

ii. Analisar os aspectos técnicos de todo e qualquer produto ou serviço de terceiros que a Brunel esteja considerando contratar para tratar dados pessoais (exemplos: nuvem, hardware, equipamentos de rede);

iii. Implementar medidas, procedimentos, controles e rotinas necessários e apropriados para manutenção da confidencialidade, integridade e disponibilidade dos dados pessoais;

iv. Coletar e manter registros das atividades de tratamento de dados pessoais; e

v. Investigar incidentes de segurança e propor medidas de remediação e mitigação em conjunto com a Brunel.

Adicionalmente, compete a área de TI da Brunel realizar testes e varreduras periódicos para detecção de vulnerabilidades e mecanismo de proteção contra softwares maliciosos. Nestes testes é registrada a análise da causa e do impacto, bem como o controle dos efeitos de incidentes de segurança para as atividades da Brunel que abrangem inclusive informações recebidas de empresas prestadoras de serviços e parceiros.

2.3. DIRETORIA DA BRUNEL

Compete à Diretoria da Brunel:

i. Analisar e tomar decisões dos relatórios realizados e informações enviadas pelo DPO; e

ii. Garantir o direcionamento e suporte da gestão para as iniciativas voltadas à garantia da privacidade e proteção de dados pessoais na Brunel.

2.4. GESTORES

Compete aos gestores da Brunel:

i. Consultar o DPO em caso de mudanças de finalidades de tratamento de dados pessoais;

ii. Realizar e manter atualizado o mapeamento dos fluxos de dados pessoais;

iii. Assegurar que qualquer dado pessoal só poderá ser tratado de acordo com as atividades profissionais autorizadas pela Brunel e nos termos desta Política e de seus documentos internos;

iv. Identificar e avaliar riscos relacionados à proteção de dados pessoais em suas atividades e propor melhorias;

v. Submeter à análise do DPO todo novo processo, incluindo novas aplicações, serviços, produtos, dentre outros, onde houver tratamento de dados pessoais; e

vi. Ao identificar violações de dados pessoais ou qualquer ação duvidosa, comunicar o DPO imediatamente.

2.5. COLABORADORES

Compete aos demais colaboradores da Brunel:

i. Cumprir as diretrizes desta Política e seus documentos complementares;

ii. Tratar os dados pessoais sob responsabilidade da Brunel somente para fins autorizados, de forma ética e legal, respeitando os direitos do Titular e de acordo com as orientações desta Política, demais instrumentos regulamentares relacionados à proteção de dados pessoais e da legislação aplicável;

iii. Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou

compartilhando indevidamente estes dados pessoais, em qualquer local ou mídia, inclusive na Internet;

iv. Reportar formalmente ao DPO quaisquer eventos relativos à violação ou possibilidade de violação de dados pessoais ou atividades suspeitas de que tiver conhecimento.

3. SUPORTE E OPERAÇÃO

Mantemos medidas técnicas e organizacionais de segurança para garantir um nível de segurança adequado à exposição de risco de nossos serviços e dados no escopo desses serviços.

Classificamos as informações com base em sua criticidade, olhando para o impacto dos negócios e do cliente sobre a violação de um ou mais fatores de confidencialidade, integridade e disponibilidade em relação a essas informações. Com base em seu nível de classificação (público, interno, confidencial, secreto), as informações são tratadas, processadas, armazenadas ou descartadas com proteção de segurança adequada aplicada, como criptografia, anonimização, período específico de retenção, entre outros.

3.1. CONTROLE DE ACESSO

Os direitos de acesso são concedidos com base nas funções de trabalho e seguindo os princípios de menor privilégio e necessidade de negócio. A necessidade de saber restringe o acesso a informações confidenciais apenas àqueles que são essenciais para cumprir a função de trabalho do usuário.

3.2. GERENCIAMENTO DE INCIDENTES

Compete à Área de TI assegurar que todos os sistemas, serviços e equipamentos usados para o tratamento de dados pessoais estejam dentro de um padrão aceitável de segurança.

Na ocorrência de qualquer incidente, deverão ser realizadas ações buscando a remediação ou a restauração dos recursos comprometidos e, quando possível, a recuperação de tais recursos ao estado anterior ao incidente.

A Área de TI deverá avaliar a gravidade do incidente, indicando se pode acarretar risco ou dano relevante aos titulares de dados pessoais. Caso haja tal possibilidade, os titulares afetados no incidente deverão ser comunicados nos termos do § 1º do artigo 48 da LGPD, conforme aplicável.

3.3. GESTÃO DE DESCARTE

Todo tratamento de dados pessoais possui um processo de gestão do descarte de informações, o qual garanta que Brunel só armazene dados pelo tempo necessário ou consentido, no âmbito e limites técnicos das atividades.

O descarte das mídias que possuam dados pessoais sensíveis deverão ser definidos pela Área de TI, para assegurar que o processo seja realizado com garantias contra acesso não autorizado ou uso impróprio.

4. TREINAMENTOS

Podemos repetir ou realizar novos treinamentos aos nossos colaboradores anualmente ou sempre que julgarmos necessário, de modo a assegurar o entendimento a respeito desta Política ou de outras boas práticas de proteção e segurança de dados e privacidade.

5. SANÇÕES

A violação de controle de segurança ou o não cumprimento das diretrizes é considerada infração e poderá implicar em medidas disciplinares (sanções) a serem validadas pela Diretoria da Brunel, conforme sua natureza e enquadramentos previstos nas leis vigentes.

6. DISPOSIÇÕES GERAIS

Esta Política deve ser revisada anualmente ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da Brunel.