MANUAL DE BOAS PRÁTICAS PRIVACIDADE E PROTEÇÃO DE DADOS (LGPD)

Santos Bevilaqua Advogados

Sumário

1. Objetivo

Este Manual de Boas Práticas atua como guia norteador para os colaboradores do Santos Bevilaqua Advogados, balizando as operações de tratamento de dados pessoais em conformidade com o preconizado pelo art. 50 da LGPD. Longe de se limitar ao cumprimento estrito da lei, a implementação dessa governança solidifica o valor institucional da banca, evidenciando o zelo na manutenção de suas políticas de conformidade. Sob essa premissa, o documento detalha os requisitos da LGPD e as atribuições dos gestores na supervisão de seus times, buscando instituir uma sólida mudança cultural. Essa evolução apoia-se na autorresponsabilidade do corpo funcional perante o fluxo de dados, assegurando a perenidade das ações de segurança da informação.

2. Papéis e Atribuições

No âmbito do tratamento de dados pessoais, cada agente que interage com as informações armazenadas e em trânsito desempenha uma função estratégica e categorizada, conforme detalhado a seguir:

⇒ Titular (Pessoa Natural): Indivíduo a quem se referem os dados pessoais que são objeto de tratamento (tais como clientes, integrantes do corpo funcional ou prestadores de serviços);

⇒ Controlador: Agente a quem competem as decisões primordiais sobre o tratamento dos dados pessoais (como a determinação de sua finalidade, compartilhamento ou descarte). No contexto das operações internas e contratos do escritório, o Santos Bevilaqua Advogados atua nesta condição;

⇒ Operador: Pessoa natural ou jurídica que efetua o tratamento de dados pessoais em estrita observância às ordens e diretrizes emanadas pelo Controlador (a exemplo de fornecedores de sistemas ou parceiros homologados);

⇒ Encarregado pelo Tratamento de Dados (DPO): Profissional ou comitê indicado pelo Controlador para atuar como canal de comunicação entre a instituição, os

titulares e a Autoridade Nacional de Proteção de Dados (ANPD), além de monitorar a conformidade interna.

3. Gestão e Ciclo de Vida dos Dados Pessoais

Esta seção detalha as premissas fundamentais da governança de dados, compreendendo as etapas de seu ciclo de vida, os ambientes de armazenamento, as diretrizes de segurança e as melhores práticas voltadas à prevenção de incidentes e vazamentos.

Sob a ótica regulatória, o armazenamento de dados pessoais não deve ocorrer de maneira indeterminada. Toda informação coletada atrela-se a uma finalidade legítima e específica, devendo ser eliminada mediante requisição do titular ou após o encerramento do tratamento, como no término de um vínculo contratual. Configura-se, assim, um fluxo temporal delimitado por critérios estritos de descarte e legislações vigentes. Paralelamente, sob o prisma da gestão documental, esse ciclo divide-se em três etapas essenciais: a produção, a utilização e a destinação final (seja por meio da eliminação segura ou da guarda permanente).

4. Ambientes de Armazenamento

As informações institucionais e dados pessoais podem estar alocados tanto em repositórios físicos quanto digitais. Isso abrange ambientes de computação em nuvem, servidores locais, correio eletrônico, sistemas internos e dispositivos móveis (como *smartphones* e *tablets*), sejam eles ativos corporativos ou individuais autorizados.

5. A Fundamentação para a Proteção de Dados

A necessidade de proteção decorre do fato de que os dados pessoais são reflexos da personalidade e privacidade do indivíduo, possuindo, ademais, expressivo valor mercantil no cenário de inteligência de negócios. Recomenda-se, portanto, prudência e criticidade quanto ao compartilhamento de dados em relações de consumo cotidianas, estimulando a compreensão dos direitos conferidos pela legislação.

6. Protocolos Preventivos e Cultura Organizacional

A segurança da informação no Santos Bevilaqua Advogados é sustentada por defesas tecnológicas robustas, incluindo criptografia, firewalls e controle de malwares. Contudo, o fator humano é o elo indispensável para a integridade do sistema. O investimento em tecnologias de ponta é complementado por programas de capacitação, assegurando que colaboradores e gestores alinhem suas condutas práticas aos princípios de proteção à privacidade. A segurança, em última análise, é uma responsabilidade coletiva.

7. Boas Prática para Gestão dos Dados

7.1. Deveres e Responsabilidades dos Colaboradores

No exercício de suas funções, compete a cada colaborador do Santos Bevilaqua Advogados zelar pela conformidade regulatória, observando estritamente os seguintes preceitos:

⇒ Atuar preventivamente para impedir a ocorrência de quaisquer prejuízos ou danos aos titulares e a terceiros em decorrência das atividades de tratamento de dados (Princípio da Prevenção);

⇒ Abster-se de utilizar ou processar informações para finalidades discriminatórias, ilícitas, abusivas ou em desconformidade com os preceitos éticos (Princípio da Não Discriminação);

⇒ Adotar condutas e controles eficazes que permitam demonstrar e comprovar a aderência prática às normas internas e à legislação de proteção de dados (Princípio da Responsabilização e Prestação de Contas);

⇒ Assegurar que o manuseio das informações restrinja-se exclusivamente às finalidades legítimas previamente informadas e consentidas pelo titular (Princípio da Adequação).

7.2. Diretrizes para a Prevenção de Incidentes e Vazamento de Dados

A incorporação de hábitos preventivos na rotina corporativa constitui o pilar fundamental para mitigar riscos de segurança. Os colaboradores do Santos Bevilaqua Advogados devem observar estritamente as seguintes práticas de governança documental e digital:

⇒ Fragmentar ou picotar de forma irreversível qualquer documento físico antes do descarte, impossibilitando a leitura de dados sensíveis;

⇒ Não deixar relatórios, listagens ou documentos contendo dados pessoais expostos sobre mesas, estações de trabalho ou impressoras e máquinas de cópia;

⇒ Abster-se do uso de documentos antigos, ordens de serviço, registros de atendimento ou cópias de documentos de identificação (como RG, CPF e CNH) como papel de rascunho;

⇒ Manter todos os documentos institucionais salvos exclusivamente nos servidores e ambientes de rede oficiais do escritório, mitigando riscos de perda e acessos não autorizados em discos locais.

⇒ Auditar regularmente as concessões de acesso em pastas de trabalho, garantindo que as informações fiquem restritas exclusivamente a quem precisa delas para o cumprimento de suas atribuições profissionais.

⇒ Abster-se do uso de aplicativos de mensagens instantâneas (sejam em contas corporativas ou pessoais) para o envio de relatórios e arquivos institucionais sensíveis sem a devida blindagem de segurança;

⇒ Jamais transferir arquivos contendo dados pessoais a terceiros alheios às atividades legítimas do escritório sem a prévia e formal validação da governança.

7.3. Boas Práticas em Ambiente Virtual

Considerando o cenário de riscos cibernéticos e a necessidade de proteção aos ativos digitais, os colaboradores deve observar rigorosamente os seguintes protocolos de segurança:

⇒ Senhas Fortes e Rotativas: Atualizar senhas de acesso regularmente, utilizando padrões complexos (letras maiúsculas/minúsculas, números e caracteres especiais);

⇒ Autenticação Multifator: Ativar obrigatoriamente o segundo fator de autenticação em todas as ferramentas disponíveis;

⇒ Desconfiar de solicitações de dados por telefone ou e-mail, mesmo que o emissor confirme dados básicos de identificação. Não interaja com mensagens suspeitas ou promoções atípicas;

⇒ Limitar a exposição de microfones e câmeras fora de reuniões operacionais, manter sistemas de proteção (antivírus) atualizados e recusar a instalação de softwares não autorizados;

8. Canais de Comunicação e Suporte

A Política de Privacidade institucional pode ser consultada na íntegra por meio do endereço eletrônico: santosbevilaqua.com.br/politica-de-privacidade .

Para esclarecimento de dúvidas, reportar incidentes ou acionar os responsáveis pela governança da LGPD no âmbito do Santos Bevilaqua Advogados, utilize o canal oficial de atendimento: suporte@santosbevilaqua.com.br