POLÍTICA DE GESTÃO DE TERCEIROS

digiteam
LEAD THE WAY

SUMÁRIO

Sumário

FOLHA DE CONTROLE

Título do documento	Política de Gestão de Terceiros
Número da versão	1.0/2024
Status	Aprovado
Setor Aprovador	Administrativo
Data da Aprovação	29/02/2024
Área responsável pela elaboração	Administrativo com auxílio de jurídico terceirizado
Área de aplicação	Brasil
Classificação da Publicidade	Externo
Controlador Responsável	DIGITEAM TECNOLOGIA LTDA (DIGITEAM)
CNPJ	07.821.585/0001-50

1. OBJETIVO

Esta **Política de Gestão de Terceiros** (a "**Política**") tem como objetivo estabelecer diretrizes claras e práticas para a contratação de parceiros comerciais que prestam serviços para o **DIGITEAM**, representam seus interesses e/ou atuam em seu nome. Esta Política é essencial para garantir que os dados pessoais sejam tratados de maneira ética, legal e segura durante todo o seu ciclo de vida.

2. ABRANGÊNCIA E APLICABILIDADE

Esta **Política** tem aplicação imediata a partir da sua publicação e deverá ser seguida por todos os colaboradores, fornecedores, terceiros e quaisquer outras pessoas, sejam físicas ou jurídicas, que tenham ou venham a armazenar e/ou eliminar dados de propriedade e/ou tratados pelo **DIGITEAM**.

O seu descumprimento será considerado **falta grave**, podendo resultar na aplicação de sanções, incluindo a rescisão do contrato.

3. LOCAL E DISPONIBILIDADE

Este documento está disponível para consulta em formato digital em: Política de Gestão de Terceiros

4. DEFINIÇÕES IMPORTANTES

LEI GERAL DE PROTEÇÃO DE DADOS ("LGPD"): Diploma normativo brasileiro (Lei nº 13.709, de 14 de agosto de 2018) que dispõe sobre o tratamento de dados pessoais em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado.

DADOS PESSOAIS: Dado relacionado a pessoa natural identificada ou identificável, tais como nome, endereço, CPF, RG, e-mail, padrões de comportamento, entre outros.

DADOS PESSOAIS SENSÍVEIS: 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.

TITULAR DE DADOS PESSOAIS ("TITULAR"): Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

TERCEIROS: São considerados terceiros, para fins desta Política, as pessoas jurídicas que possuem relações negociais e operações com o DIGITEAM, tais como prestadores de serviços, parceiros, fornecedores e outros profissionais que possuam relação comercial com a empresa.

TRATAMENTO DE DADOS PESSOAIS ("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, controle da informação, modificação, comunicação, transferência, difusão ou extração.

ENCARREGADO: também conhecido como DPO (Data Protection Officer). É a pessoa indicada por nós para atuar como canal de comunicação entre os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais em todo território nacional.

CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

5. ORIENTAÇÕES DE TRATAMENTO DE DADOS PESSOAIS DE REPRESENTANTES DE PARCEIROS COMERCIAIS DO DIGITEAM

Durante o relacionamento do DIGITEAM com o terceiro, é possível que haja o tratamento de dados pessoais de representantes dos terceiros, em razão das atividades desempenhadas pela nossa empresa e/ou pela natureza da relação que tivermos com o terceiro. Esses tratamentos de dados devem ser pautados pelas seguintes orientações:

Despessoalização da prestação do serviço: sempre que possível, dados de prestadores de serviços e fornecedores de produtos com relação comercial com a empresa devem ser dados corporativos e não dados pessoais.

Mínimo necessário: o tratamento de dados pessoais deve ser limitado ao mínimo necessário para o objetivo para o qual eles existem.

Confidencialidade: as informações compartilhadas em razão do vínculo comercial devem ser mantidas em caráter sigiloso e confidencial, sempre que necessário.

Segurança da informação: os dados pessoais devem ser protegidos contra perda, modificações não autorizadas e acessos indevidos.

Compartilhamento de dados limitado ao mínimo necessário: os dados pessoais do terceiro compartilhados para execução de serviços pelo terceiro devem ser limitados ao mínimo necessário à boa e correta prestação dos seus serviços.

6. DIRETRIZES GERAIS DE ESCOLHA, VÍNCULO E DESENVOLVIMENTO DE ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS POR EMPRESAS PARCEIRAS COMERCIAIS

- A existência de um Projeto de Adequação/Programa de Gestão da Privacidade é considerada fundamental para escolha de propostas comerciais de agentes parceiros, sendo considerado critério de desempate entre agentes.

- É obrigatório avaliar se o terceiro age em cumprimento da legislação, da regulamentação e recomendações relacionadas à proteção de dados pessoais, em especial da Lei Geral de Proteção de Dados Pessoais (a Lei Federal nº 13.709/2018, a "LGPD") e se aplica as medidas adequadas de segurança para garantir a confidencialidade, integridade, acessibilidade responsável, rastreabilidade de operações e autenticidade de dados pessoais, quando:
    - A natureza do vínculo com o terceiro demandar a análise das suas operações de forma mais aprofundada;
    - A categoria de titulares afetados pelo compartilhamento for relevante;
    - O tipo de dados pessoais compartilhados entre as partes forem sensíveis e/ou de grande impacto à privacidade dos titulares;
    - O tratamento for baseado no legítimo interesse do DIGITEAM;
    - A forma de tratamento for baseada em novas tecnologias e/ou redes neurais.

- Caso seja necessário em razão de obrigação legal, contratual ou complexidade da estrutura organizacional do terceiro ou do tipo de dados pessoais que ele trata, ter um Encarregado de Tratamento de Dados Pessoais é fundamental que apresente um Encarregado de Tratamento de Dados Pessoais (DPO).

- No contrato, deve constar cláusula sobre a condição de Controlador ou de Operador ou de Sub Operador de cada parte envolvida.

7. REGISTROS

Deverá ser mantido o Formulário de Adequação do Anexo I para avaliação, controle e monitoramento interno do status de proteção de dados pessoais e da privacidade pelos terceiros.

Poderá ser requerido do terceiro o preenchimento do Anexo II para avaliação da conformidade com as legislações aplicáveis, quando o gestor entender necessário.

8. REVISÃO E ATUALIZAÇÃO

Esta Política será revisada e atualizada periodicamente, a critério do DIGITEAM, em razão de eventuais modificações de procedimentos internos e/ou exigências legais ou regulatórias sobre proteção de dados pessoais.

HISTÓRICO		
Versão	**Alterações**	**Data**
1.0	Disponibilização	29/02/2024

ANEXO 1 – Formulário de Adequação – Privacidade e Proteção de Dados - SIMPLIFICADO

Razão social:			
Ramo de atividade:			
Nome e cargo do responsável pelo preenchimento:			
Telefone/e-mail:	Data:		
Itens de verificação			
1	A empresa possui Política de Privacidade? (anexar)	Sim	Não
2	A empresa possui Política de Segurança? (anexar)		
3	A empresa possui Código de Conduta? (anexar)		
4	A empresa possui Acordo de Confidencialidade e não divulgação? (anexar)		
5	A empresa nomeou um Encarregado de Proteção de Dados? (informar identidade e canal de contato)		
6	A empresa possui um Comitê de Proteção de Dados e Privacidade?		
7	A empresa possui protocolo para resposta a incidentes?		
8	A empresa possui protocolo de atendimento a direitos de titulares?		

ANEXO 2 – Formulário de Adequação – Privacidade e Proteção de Dados – COMPLETO

Domínio	Requisito	Atende 0 - Não 1 - Sim	Requisito obrigatório	Peso	Nota
Governança | Privacidade de Dados	Conscientiza, dissemina e compromete toda a empresa com as iniciativas de adequação a LGPD				
	Registra, organiza e mantém atualizada toda a documentação relativa ao processo de conformidade com a privacidade de dados				
	Realiza avaliações dos colaboradores, sobre conhecimento à LGPD e os processos de privacidade de dados da empresa				
	Acompanha e demonstra os níveis de conformidade junto aos executivos da empresa				
	Implementa cultura de Privacy By Design no ambiente da empresa				
	Audita processos de privacidade de dados na empresa com periodicidade definida				
	Audita, avalia e mitiga riscos associados a fornecedores críticos				
	Implementa políticas, normas e processos de continuidade de negócio				
	Realiza mapeamento e inventário de dados pessoais				
	Realiza documentação e manutenção de fluxo de dados pessoais				

Proteção de Dados	Realiza classificação dos ativos, processos e dados (Ex. público, confidencial, restrito, sigiloso)				
	Mantém mapeamento, inventário e classificação de dados atualizado				
	Implementa controles de Segurança da Informação para proteção direta dos dados, tais como Firewall de Banco de dados, controle de acesso, gerenciamento de logs, correlação de logs				
	Implementa controles de Segurança da Informação para proteção de acesso direto aos dados pessoais e sensíveis, por ferramentas de manipulação de dados				
	Implementa processo de restrição de acesso a dados pessoais e sensíveis				
	Implementa controles de Segurança da Informação para acesso às aplicações que manipulam os dados				
	Implementa processo de anonimização de dados, aos dados pessoais e sensíveis e/ou exclusão de dados pessoais ao final do tratamento				
	Implementa objetivos de minimização de dados pessoais				
	Implementa controles de Segurança da Informação para proteção de perímetro, evitando acessos indevidos à rede de comunicação da organização, tais como Firewall de perímetro, WAF, IPS				
	Realiza conscientização, educação e treinamento em segurança da informação				

	Implementa processo de segurança em escritórios, salas e instalações				
	Possui política de mesa limpa e tela limpa				
	Possui controles contra malware				
	Gerencia cópias de segurança das informações				
	Possui controles criptográficos				
	Possui transferência internacional de dados pessoais				
	Possui registros de dados pessoais divulgados para terceiros				
	Há certificação de ISO 27001 para processos críticos e core da organização				
Titulares de Dados	Gerencia consentimentos dos titulares de dados				
	Gerencia e atender os direitos dos titulares				
	Disponibiliza canal de atendimento aos titulares (indicar o canal)				
	Informa aos titulares quais dados são coletados e as ações executadas com cada um destes dados				
	Possui avaliação de riscos de segurança da informação				
	Gerencia e responder a incidentes e violações de privacidade com política, normas e procedimentos estabelecidos				

Resposta a Incidentes	Realiza treinamento de resposta a incidentes junto aos colaboradores de TI, SI e áreas de negócio				
	Possui protocolo para aprender com os incidentes de segurança da informação				
	O Comitê de Proteção de Dados Pessoais realiza reuniões de trabalho com frequência definida				
	É capaz de monitorar intrusões suspeitas na rede				
	É capaz de identificar se um ataque está ocorrendo				
	É capaz pode isolar o ataque e restringir danos potenciais				
	É capaz de saber se dados confidenciais da organização estão sendo compartilhados de forma não autorizada				
	Há um plano formal de gerenciamento de crises em prática, testado e alinhado ao risco organizacional				
	Tem habilidades e conhecimentos forenses para atuar no incidente				

Descreva de forma resumida quais são as medidas técnicas, administrativas e de segurança utilizadas na empresa para a proteção dos dados pessoais: