[POLÍTICA CORPORATIVA DE PROTEÇÃO DE DADOS PESSOAIS]

RESUMO DO DOCUMENTO

Título: Política corporativa de proteção de dados pessoais

Número: ------

Versão: 01

Classificação do documento: Uso interno

Vigência: 24 meses

Data de revisão: 16/06/2023

Elaborador por: Gerência de Processos e Operações e Jurídico

Aprovado por: Conselho de Sócios

SUMÁRIO

OBJETIVO

Prezados colaboradores, parceiros, clientes e fornecedores,

A proteção de dados no processamento de informações de nossos clientes e consumidores representa hoje um dos grandes ativos a serem cuidados em nossa estrutura, sobretudo pelo aumento de exigências normativas e expectativas naturais do mercado.

A Sistemas TH recomenda a todos os seus parceiros, colaboradores, clientes e fornecedores um elevado nível de comprometimento para cumprimento das regras desta Politica Corporativa, para que tenhamos uniformidade e um elevado nível de proteção dos dados que de alguma forma sejam tratados pela Sistemas TH. Um tratamento cuidadoso desses dados corresponde à expectativa de nossos clientes e parceiros de negócios e é a base para uma relação comercial de confiança.

Essa diretriz determina um padrão para o processamento dos dados pessoais de nossos interessados, clientes e parceiros de negócios, o qual se baseia nas exigências legais e em princípios de proteção de dados, principalmente em relação a Lei Geral de Proteção de Dados Pessoais, Lei 13.709/18

Portanto, a presente Política tem como objetivo a criação de condições básicas necessárias para um intercâmbio de informações intrínseco ao cumprimento do objetivo social da Sistemas TH, uma vez que garantir o nível adequado de proteção de dados, igualmente, é de interesse de todos parceiros comerciais

A. DEFINIÇÕES

Cliente: Pessoa Jurídica, contratante dos serviços da Sistemas TH.

Dado Pessoal: Toda e qualquer informação que, isolada ou conjuntamente com outras informações fornecidas, permitam a identificação e individualização de quem as forneceu.
É considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

Dado Sensível: Dados pessoais sobre a origem racial ou étnica, convicções religiosas, dados referentes à saúde, à vida sexual, além de dados genéticos e biométricos.

Dado Anonimizado: Dados relativos a um titular que não possa ser identificado.

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.

Banco de dados: Conjunto estruturado de dados pessoais em formato eletrônico ou físico.

Titular de dados: Pessoa natural a quem se referem os dados pessoais objeto de tratamento.

Controlador: Pessoa natural ou jurídica a quem compete as decisões sobre tratamento de dados pessoais.

Operador: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para a finalidade informada.

Uso compartilhado dos dados: A comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Violação de dados pessoais: Uma violação da segurança, acidental ou ilícita, que consista na destruição, perda, alteração, divulgação ou no acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

B. PRINCÍPIOS PARA O PROCESSAMENTO DE DADOS PESSOAIS

Todo tratamento de dados deverá sempre observar os princípios abaixo elencados:

Finalidade: Realizar o tratamento com vistas a atender propósitos legítimos, específicos, explícitos, de acordo com o estipulado pelo Controlador, de modo que qualquer tratamento posterior em dissonância com a finalidade divulgada será vedado. Os dados pessoais não deverão ser guardados para eventuais finalidades futuras, exceto se se tratar de obrigação legal;

Adequação: Realizar o tratamento de forma compatível com a finalidade estipulada pelo Controlador;

Necessidade: Limitar o tratamento ao necessário à consecução da finalidade estipulada, de modo que diante o atingimento desta, os dados deverão ser eliminados, tendo em conta as obrigações existentes de armazenagem;

Transparência: Garantir ao encarregado determinado pelo Controlador (Cliente) informações claras e precisas sobre o tratamento de dados realizado, resguardados os segredos comerciais;

Qualidade Dos Dados: Garantia ao encarregado determinado pelo Controlador (Cliente) acerca da exatidão, clareza, relevância e atualização dos dados, conforme a necessidade e finalidade do tratamento;

Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Não discriminação: Impossibilidade de tratamento de dados para fins discriminatórios ilícitos ou abusivos;

Responsabilidade e prestação de contas: Demonstração acerca da adoção de medidas eficazes e capazes de comprovar o cumprimento e observância das regras estabelecidas nesta política, inclusive a eficácia das medidas.

C. NÃO APLICAÇÃO

Esta Política Corporativa não se aplica a análises estatísticas ou inspeções efetuadas com base em dados anonimizados.

D. POLÍTICAS ESTABELECIDAS

D1. Diretrizes gerais

Os dados pessoais coletados ou recebidos pela Sistemas TH de funcionários, candidatos a vagas de emprego,

possíveis clientes, consumidores dos clientes, parceiros de negócios devem ser mantidas em banco de dados especifico, com acesso restrito.

A coleta dados pessoais é realizada para legitimar relações administrativas e comerciais, tais como: pesquisas internas de marketing; administração de segurança e desempenho; informações de contato; recursos humanos; viabilização de negócios e prestação de serviços entre outras finalidades que forem estipuladas entre a Sistemas TH e seus empregados, parceiros, clientes e fornecedores.

A Sistemas TH utilizará os dados de forma consistente com esta política e com a lei em vigor. Todas as informações pessoais coletadas ou recebidas serão utilizadas para fins legitimamente de negócios.

D2. Coleta/uso de dados

A coleta e uso de dados pessoais deverá se basear em uma destas hipóteses:

- Consentimento (escrito ou por meio que demonstre a vontade do titular);
- Obrigação legal;
- Necessidade para execução contratual;
- Exercício regular de um direito;
- Proteção à vida ou incolumidade física do titular ou de terceiro;
- Para a tutela da saúde;
- Para atender a legítimo interesse do controlador (cliente) ou terceiro;
- Para a proteção de crédito;
- E e m razão da publicidade dada aos dados por seu titular ou do acesso público a este.

D2.1 Uso de informações de criança

A Sistemas TH entende como relevante e sensível os dados pessoais de crianças. Desta forma, esta opta por não receber ou tratar dados de crianças (pessoas com até 12 anos incompletos), sendo assim, caso sejam enviados à Sistemas TH dados de crianças estes deverão vir acompanhados do registro de consentimento expresso de ao menos um dos pais ou responsável.

D3. Propósito para utilização dos dados pessoais

Os dados pessoais, coletados ou recebidos pela Sistemas TH, devem ser utilizados para fins relacionados à área de recursos humanos da Sistemas TH ou à prestação de serviço, delimitados em Contrato específico.
O compartilhamento de dados com parceiros só poderá ser realizado mediante prévia autorização da Gestão de Processos e Operações.
O uso de dados de acesso público ou tornados públicos pelo titular observará à finalidade
com que foram disponibilizados, a boa-fé e os direitos fundamentais dos titulares.

D3.1 Classificação das informações pessoais a serem utilizadas

Todas informações pessoais coletas, tratadas e compartilhadas, em qualquer formato, devem ser classificadas pelo responsável pelo seu tratamento, observados os critérios ora criados e legislação nacional vigente, sendo certo que a sua classificação delimitará seu uso/finalidade e tratamento.

A classificação é segmentada nos três tipos de informação a seguir expostos:

#confidencial

Informações que possam influenciar o microambiente, no qual a Sistemas TH está inserido. São informações que devido a sua potencialidade deverá ser amparada pelo sigilo empresarial e comercial.

#interna

São as informações protegidas por alguma hipótese legal de sigilo, como comercial, profissional, industrial e segredo de justiça.

#pública

Informações que podem ser divulgadas sem restrições de acesso, observadas as conveniências do processo, produto ou serviço a que diz respeito.

D.3.2 Critérios de tratamento da informação

Toda informação compartilhada ou veiculada deve ser classificada conforme a segmentação delimitada acima e conforme os critérios abaixo delineados:

Informação em uso	#Confidencial	#Interna
Malote (entre dependências)	Utilizar duplo envelopamento, informando previamente ao destinatário sobre o envio e exigindo comunicação de eventual sinal de violação do envelope	Utilizar envelopamento simples, informando previamente ao destinatário sobre o envio
Correio (serviço postal)	Uso desaconselhado. Caso necessário, recomenda-se o uso de correspondência ou remessa expressa que permita o rastreamento e aviso de recebimento.	Usar correspondência envelopada, registrada e que possa ser rastreada
Ambiente eletrônico	Utilizar canais que impossibilitem a interceptação das informações e manter registro das atividades	Utilizar canais que impossibilitem a interceptação das informações e manter registro das atividades

E-mail corporativo (destinatário interno)	Utilizar e-mail corporativo com criptografia ou sinalizar no assunto a necessidade de "manter em particular".	Exclusivamente com uso dos veículos de comunicação administrativa
E-mail corporativo (destinatário externo)	Utilizar e-mail corporativo com criptografia ou sinalizar no assunto a necessidade de "manter em particular".	Usar apenas quando houver interesse negocial, desde que autorizado pelo responsável
Mensageria, via mobile (Whatsapp, Viber, ChatOn, Line, Google+, Hangouts e outros)	Observar os veículos informativos de comunicação interna.	Observar os veículos informativos de comunicação interna.
FAX	Verificar a discagem correta do número, notificar o destinatário previamente ao envio e confirmar a recepção. Não utilizar para destinatários externos.	Verificar a discagem correta do número, notificar o destinatário previamente ao envio e confirmar a recepção.
Sítios da internet	Não é permitido. Pode-se excetuar, mediante autorização formal do responsável pela informação.	Não é permitido. Pode-se excetuar, mediante autorização formal do responsável pela informação.
Conversas em locais públicos	Vedado.	Vedado.
Reuniões	Garantir que apenas pessoas autorizadas acessem o ambiente.	Garantir que apenas pessoas autorizadas acessem o ambiente.
Telefone fixo	Precaver-se contra a aproximação de pessoas não autorizadas. Não utilizar a função viva-voz, a não ser às portas fechadas.	Precaver-se contra a aproximação de pessoas não autorizadas.
Celulares	Precaver-se contra a aproximação de pessoas não autorizadas. Não utilizar a função viva-voz, a não ser às portas fechadas.	Em locais públicos, utilizar longe de terceiros e com tom de voz moderado.
Estações de trabalho	Estabelecer controle de acesso com restrição de usuário, controle de versionamento e senhas disponíveis nas ferramentas tecnológicas. Utilizar solução de criptografia, se possível.	Utilizar controle de versionamento disponível nas ferramentas tecnológicas.
Reprodução	Cópias devem ser previamente autorizadas pelo responsável pela informação. Atentar para a integridade e confidencialidade da informação.	Permitido, desde que mantida a integridade das informações e seja para uso exclusivo no desenvolvimento das atividades profissionais.

Informação em arquivo	**#Confidencial**	**#Interna**

Impressos, formulários e anotações	Guardar em local restrito e trancado, preferencialmente em armário de segurança.	Guardar em local restrito e trancado. Disponível apenas aos que necessitam pela natureza do trabalho.
Informações eletrônicas	Armazenamento em rede corporativa e controle de acesso compatíveis com a criticidade e confidencialidade da informação.	Armazenamento em rede corporativa e controle de acesso compatíveis com a criticidade e confidencialidade da informação.
Mídias removíveis e dispositivos móveis	Utilizar criptografia, guardar em armário de segurança. Disponível apenas aos que necessitam em razão da natureza de seu trabalho.	Utilizar criptografia, guardar em local restrito e trancado. Disponível apenas aos que necessitam em razão da natureza de seu trabalho.
Demais mídias	Guardar em armário de segurança. Disponível apenas aos que necessitam em razão da natureza de seu trabalho.	Guardar em local restrito e trancado. Acesso apenas aos que necessitam em razão da natureza de seu trabalho.

Descarte/ Destruição	**#Confidencial**	**#Interna**
Impressos, formulários e anotações com ou sem o logotipo ou qualquer identificação da Sistemas TH	Utilizar fragmentadora ou qualquer outro meio, de forma a não permitir a sua recuperação.	Utilizar fragmentadora ou qualquer outro meio, de forma a não permitir a sua recuperação.
CD, DVD, Pen Drive, HD externo e dispositivos móveis	Fragmentar, perfurar, picotar ou destruir, de forma a não permitir sua recuperação.	Fragmentar, perfurar, picotar ou destruir, de forma a não permitir sua recuperação.

D4. Segurança

Conforme contrato padrão estabelecido entre a Sistemas TH e os Controladores (Clientes), só serão permitidos acessos através de IPs Fixos, previamente cadastrados , através de solicitação formal efetuada pelo encarregado indicado pelo Controlador (Cliente).

O Controlador (Cliente), possui logins/senhas para acesso, cuja responsabilidade de atribuição é do encarregado indicado pelo Controlador (Cliente).

Todos os dados cadastrais são armazenados em banco de dados e criptografados, com acesso restrito através de login/senha.

D5. Retenção das informações

A SISTEMAS TH não retém informações recebidas e retornadas dos Controladores (Clientes). Os dados pessoais de usuários são armazenados, conforme previsto no item D4 deste documento, durante o tempo necessário para atender os objetivos previamente contratados com o Controlador (Cliente). Quando solicitado pelo Controlador (Cliente), a exclusão dos dados do titular deverá ser realizada imediatamente, se for o caso.

D6. Compartilhamento de Dados pelos Controladores (Clientes e Parceiros) com a Sistemas TH (Operador)

O compartilhamento de dados pessoais por parceiros com a Sistemas TH e desta com os Controladores (Clientes) e vice-versa se dará por questões relacionadas ao objeto estabelecido em Contrato, devendo o Controlador (Parceiro ou Cliente), possuir a evidência de conhecimento e consentimento do titular, dono da informação, acerca da destinação desta.

Todos os Controladores (Clientes e Parceiros) se comprometem contratualmente a adotar medidas de segurança de nível similar ou superior aos da Sistemas TH.

D7. Privilégios e responsabilidades no acesso a dados pessoais

Todos os colaboradores com acesso direto a dados pessoais na empresa, seja em atividades de coleta, armazenamento, tratamento ou qualquer outro uso, são identificados de forma individual através de login/senha, além de terem seus acessos limitados as necessidades de suas atividades dentro da Sistemas TH. Além desta politica, os colaboradores devem observer as normas contidas nos seguintes documentos:

. Normas Gerais de Seguranca da Informação;
. Norma Utilização de Internet e Correio Eletrônico;
. Utilização e Monitoramento dos Recursos de Informação;
Trimestralmente o processo de Privilégios e responsabilidades no acesso a dados pessoais é analisado e avaliado.

A Sistemas TH mantém registro detalhado de todos os acessos aos dados, contendo as seguintes informações: Data, Horário de inicio e término, usuário e chave de acesso.

D8. Conformidade e legalidade

Todas as áreas de negócio, parceiros, colaboradores e terceiros da Sistemas TH, devem estar em conformidade com as leis e regulamentações vigentes e com os padrões de segurança estabelecidos pela Sistemas TH.

D9. Respeito aos direitos dos titulares de dados

A Sistemas TH como figura do Operador exige em seus contratos com Parceiros e Clientes(Controladores) que estes devem garantir diretamente ou contratualmente, por meio de Parceiros e Clientes, mediante requisição, os seguintes direitos dos titulares de dados: (i) confirmação de existência de tratamento dos dados; (ii) acesso aos dados; (iii) correção de dados; (iv) anonimização e eliminação dos dados; (v) portabilidade dos dados, resguardados os segredos comerciais; (vi) informação sobre a possibilidade de revogação/retirada do consentimento; (vii) revogação do consentimento.

E. RESOLUÇÃO DE LITÍGIOS

Qualquer dúvida ou preocupação com relação ao uso ou divulgação de Informações pessoais deve ser encaminhada a Gestão de Processos e Operações. Caso não haja satisfação por parte do autor da denúncia/reclamação em relação à decisão proferida, este deverá recorrer ao Conselho de Sócios.

F. INCIDENTE DE DADOS

Caso seja detectado qualquer violação de dados pelas áreas de negócio, parceiros, clientes, colaboradores e terceiros da Sistemas TH, este deverá ser informado a Gestão de Processos e Operações, imediatamente após conhecimento do ocorrido, a menos que seja capaz de demonstrar que esta violação não é suscetível de implicar em risco para os direitos e garantias individuais dos titulares de dados envolvidos. Se não for possível efetuar esta comunicação imediatamente, a notificação deverá ser dar em até 48h, acompanhada dos motivos de atraso, podendo as informações serem fornecidas por fases sem demora injustificada.

A Comunicação deverá descrever: (i) a natureza da violação de dados (indicando categorias dos dados); (ii) as informações sobre os titulares de dados envolvidos; (iii) descrição das prováveis consequências.

A Gestão de Processos e Operações irá analisar a comunicação e, se for o caso, tomar as medidas legais cabíveis junto à autoridade competente.

G. ELABORADOR DA POLITICA

Gestão de Processos e Operações / Juridico

H. APROVADORES

Sócios-Diretores

I. PERÍODO DE VIGÊNCIA

Esta política tem vigência por prazo indeterminado.

Ciente e De acordo:

São Paulo, de de .

_____

Nome:
CPF:
RG: