

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 17 de março de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Empresa Desenvolvedora do Sistema.

Operador(es): Empresa Adquirente do Sistema.

Encarregado: Escritório contratado pela empresa desenvolvedora do sistema.

E-mail do(s) Encarregado(s): (cesar.psgjunior@gmail.com)

2 - NECESSIDADE DE ELABORAR O RELATÓRIO

Atendimento ao artigo 5o, inciso II, artigo 10, parágrafo 3o., artigo 14, artigo 42 todos da Lei 13.907/2018 - Lei Geral de Proteção de Dados.

3 - DESCRIÇÃO DO TRATAMENTO

Relativamente à natureza, escopo, contexto e finalidade do tratamento, a CONTROLADORA informa que, diante de sua atividade principal de desenvolvimento de sistemas digitais, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

- a) Registra e processa dados pessoais e sensíveis relativos à documentação do TITULAR como: nome, e-mail, endereço e telefone do TITULAR, para identificação do TITULAR no contexto da empresa.
- b) Registra e processa dados pessoais e sensíveis relativos à documentação fiscal (CPF), nome e forma de pagamento do TITULAR, quando for identificado como cliente, quando este efetuar uma compra, e quando optar por se identificar, através do sistema de pedidos, com objetivo de registrar a venda do produto e efetuar a cobrança correta.
- c) Processa dados pessoais do TITULAR, no contexto do interesse legítimo do controlador em razão de sua responsabilidade na comunicação de dados fiscais às autoridades competentes.
- d) Processa dados que podem causar dados patrimoniais ao TITULAR, quando este identificado como cliente, referente a sigilo fiscal, bancário e tributário, para receber pagamentos relativos a produtos vendidos pela CONTROLADORA ao TITULAR.

Todos dados são coletados e tratados no contexto da venda de produtos, com a finalidade do cumprimento de obrigações fiscais e tributárias, além de obrigações acessórias exigidas pela legislação brasileira.

4 - PARTES INTERESSADAS CONSULTADAS

1. Entidades legais consultadas
 - a) Ministério público do estado de São Paulo devido sua atuação ora como passivo quando se constitui como pessoa jurídica de direito público e ativo quanto ao seu dever de garantir, no âmbito coletivo, que as determinações legais sejam cumpridas.
2. Encarregado dos dados, como citado na seção 1.
3. Especialistas de segurança da CONTROLADORA, notadamente: Tarciso Jr.; Davi M.; Flavio N.; Silvester;.
4. Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por empresa adquirente do sistema.

Todas as partes interessadas devem participar, em diferentes momentos, do processo de criação do presente documento. O time de operação de negócio participou na identificação dos dados operados, no apoio à definição do contexto de operação dos dados, e foi treinado para operar os dados de acordo com a política de dados definida.

Os especialistas de segurança preparam os relatórios técnicos que servirão de base à criação da política de dados e a este relatório. O Encarregado dos dados, junto aos representantes jurídicos do CONTROLADOR, elaboram o documento, que será posteriormente validado com as entidades competentes.

5 - NECESSIDADE E PROPORCIONALIDADE

Fundamentação legal: artigo 5o, inciso II, artigo 10, parágrafo 3o., artigo 14, artigo 42 todos da Lei 13.907/2018 - Lei Geral de Proteção de Dados.

Tendo em vista que o legítimo interesse do CONTROLADOR é uma das fundamentações em razão de sua responsabilidade solidária ao TITULAR em caso de irregularidade fiscal e tributária:

- o tratamento dos dados sensíveis, quando aplicável, é indispensável ao cumprimento das exigências da legislação tributária, fiscal e trabalhista brasileira;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito;
- o processo atual de fato auxilia no propósito almejado.

Os dados coletados com essa finalidade devem ser eliminados após o período de 5 (cinco) anos, conforme exigido pela legislação em vigor. Enquanto perdurar esse prazo, os dados devem ser criptografados, armazenados em nuvem, com segurança de implementação.

As informações de privacidade aos titulares seguem as diretrizes da obrigatoriedade de se manterem arquivadas todas as evidências fiscais, tributárias e trabalhistas de todas as informações enviadas aos sistemas oficiais da autoridade tributária brasileira, quando houver.

A entidade CONTROLADORA poderá, a pedido do TITULAR, transferir a ele a guarda de tais informações, ressalvadas àquelas que o próprio CONTROLADOR, por dever de ofício, deve possuir pelo período constante da legislação.

6 - IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Identificamos os seguintes riscos, classificados de acordo com sua probabilidade (P) e seu impacto (I). O nível de risco se dá pela multiplicação dos dois fatores. As gradações são 5 (baixo), 10 (médio) e 15 (alto).

N do Risco	Especificação do Risco	P	I	Nível de Risco
R01	Vazamento dos dados	10	15	150
R02	Acesso de edição direta aos dados	10	15	150
R03	Perda de dados por falha de software	5	10	50
R04	Indisponibilidade e do sistema de operação dos dados	5	5	25

7 - MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida	Efeito sobre o risco	Medida aprovada
R01	1. controle do acesso ao sistema.	reduzir	sim
R02	1. trava para edição dos dados via ferramentas sql.	reduzir	sim
R03	1. testes unitários e integrados devidamente documentados.	mitigar	sim

Risco	Medida	Efeito sobre o risco	Medida aprovada
R04	1. monitoramento de todos os componentes da solução	reduzir	sim

8 - APROVAÇÃO

Assinaturas:

Representantes do CONTROLADOR

Cesar.

Davi.

Tarciso.

Flavio.

Silvester.