RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 21 de julho de 2024

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Health&Med - Sistema de Telemedicina.

Operador(es): Health&Med - Sistema de Telemedicina, AMAZON AWS SERVICOS BRASIL LTDA, GOOGLE BRASIL INTERNET LTDA (Google Agenda e Google Meetings).

Encarregado: FIAP - VSTP EDUCACAO SA.

E-mail do Encarregado: pessoa.f@emflgpd.com.

Telefone: (11) 91111-2222.

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 gestão de restaurantes, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

1. Coleta e trata dados pessoais e sensíveis relativos à documentação fiscal e regulatória, bem como os dados pessoais nome e CPF do TITULAR, para identificação do TITULAR no contexto da empresa.

2. Coleta e trata dados pessoais e sensíveis relativos à documentação fiscal (CPF), endereço e nome do TITULAR, quando for identificado como cliente, e quando este efetuar uma compra através da loja eletrônica, para fins de efetuar a entrega do produto e efetuar a cobrança correta.

3. Trata dados pessoais do TITULAR, seja este identificado como cliente ou associado, no contexto do interesse legítimo do controlador em razão de sua responsabilidade na comunicação de dados fiscais às autoridades competentes.

4. Trata dados que podem causar danos patrimoniais ao TITULAR, quando este identificado como associado, referente a sigilo fiscal, bancário e tributário, para efetuar pagamentos relativos a serviços prestados pela CONTROLADORA ao TITULAR.

5. Trata dados que podem causar danos patrimoniais ao TITULAR, quando este identificado como cliente, referente a sigilo fiscal, bancário e tributário, para receber pagamentos relativos a produtos vendidos e/ou serviços prestados pela CONTROLADORA ao TITULAR.

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

4. PARTES INTERESSADAS

4.1 Entidades legais consultadas:

- Escritório Moraes & Fernandes, representado por Lispector, C., especialista em tributação no contexto da LGPD; Meireles, C., especialista em avaliação de segurança de dados pessoais no contexto da LGPD;
- Secretaria Estadual de Segurança de Dados.

4.2 Encarregado dos dados, como mencionado na seção 1

4.3 Especilistas de segurança da CONTROLADORA, notadamente:

- Joyce J;
- Cervantes M;
- Mendes Campos P.

4.4 Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA:

- Representados por Sagan C., responsável pelo treinamento e acompanhamento do time em questões de segurança de dados e quaidade da operação

Todas as partes interessadas participaram, 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 serviram de base à criação da política de dados e a este relatório. O Encarregado dos dados, junto aos representantes jurídicos do CONTROLADOR, elaboraram este documento, que foi 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 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.

Todos os dados coletados com essa finalidade são eliminados após o período exigido pela legislação, que é de 5 (cinco) anos. Enquanto perdurar esse prazo, o encarregado manterá todos os dados criptografados com chaves assimétricas, armazenados em dois fornecedores de nuvem diferentes, com segurança de nuvem e de implementação, e duplo fator de autenticação, inclusive para fins de recuperação de arquivos de segurança e recibos de transmissão e evidência de cumprimento de obrigação acessória e principal.

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.

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.

É importante constar que não há, por legislação, a retroatividade do processamento dos dados, em caso de transferência de guarda de informações. Para fins legais, o direito ao esquecimento será garantido para os dados usados em processos transacionais.

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	Especialização do Risco	P	I	Nível do Risco
R01	Acesso não Autorizado	10	15	150
R02	Operação incorreta dos dados	5	15	75
R03	Desfiguração de dados por falha de software	5	10	50
R04	Indisponibilidade do Sistema de operações dos dados	5	5	25

7. MEDIDADS PARA TRATAR OS 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).

Risco	Medida	Efeito Sobre o risco	Medida aprovada
R01	1. Controle do acesso lógico 2. Monitoramento ativo de ações suspeitas no ambiente de operação	Reduzir	Sim
R02	1. Treinamento 2. Redução de dados para operação	Reduzir	Sim
R03	1. Efetuar testes completos e documentados antes de iniciar o uso	Mitigar	Sim
R04	1. Controle de failover para falhas que causem indisponibilidade 2. Monitoramento de todos os componentes da solução	Reduzir	Sim

8. APROVAÇÃO

Assinaturas:

Representante do CONTROLADOR

Encarregado dos dados ou seu representante