RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 27 de junho de 2024

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: BOPEJS - Sistema de Gestão de Restaurantes (RMS)

Operador(es): BOPEJS - Sistema de Gestão de Restaurantes (RMS), AMAZON AWS SERVICOS BRASIL LTDA, Mercado Pago Instituição de Pagamento Ltda.

Encarregado: FIAP - VSTP EDUCACAO SA.

E-mail do Encarregado: atendimento.postech@fiap.com.br

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, com a finalidade de identificar o TITULAR ao efetuar a cobrança e entrega do produto.

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:

- João Pedro do Espirito Santo Almeida;
- Rafael Fernandes da Silva;
- Diego Luis de Oliveira.

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

- Representados por Ana Paula Lopes, responsável pelo treinamento e acompanhamento do time em questões de segurança de dados e qualidade 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, armazenado no fornecedores de nuvem, 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).

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	5	15	75
R02	Modificação não autorizada.	5	15	75
R03	Perda.	5	5	50
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	25
R06	Coleção excessiva.	5	5	25
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	150
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada etc.).	5	15	75
R14	Reidentificação de dados pseudoanonimizados.	5	15	75

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	Controle/Medida	Efeito	Risco Residual	Controle/

		sobre o Risco	P	I	Nível (P x I)	Medida(s) Aprovado s(as)
R01 Acesso não autorizado.	GESTÃO DO CONTROLE DE ACESSO: Processo de concessão e revogação de acesso; Uso de MFA. SEGURANÇA DE APLICAÇÕES: Desenvolvimento Seguro.	Reduzir	5	10	50	Sim
R04 Roubo.	GESTÃO DO CONTROLE DE ACESSO: Processo de concessão e revogação de acesso; Uso de MFA. PROTEÇÃO DE DADOS: Descarte seguro de dados; Uso de criptografia em repouso e em trânsito.	Reduzir	5	5	25	Sim
R06 Coleção excessiva.	MINIMIZAÇÃO DE DADOS: Coleta somente dos dados necessários para a finalidade; Revisão periódica dos dados pessoais coletados para alinhamento com a finalidade.	Reduzir	5	10	50	Sim

8. APROVAÇÃO

Assinaturas:

Representante do CONTROLADOR

Encarregado dos dados ou seu representante