G23 Consultoria

RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

G23 Consultoria

São Paulo, 19 de Março de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
19/03/2024	1.0	Conclusão da primeira versão do relatório	Pedro Costa

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO
Controlador
Hamburgão da Galera Lanches
Operador(es)
Ronald McDonald, Birdie, Papa-burguer, P. McCheese
Encarregado (DPO)
Pedro Costa

E-mail Encarregado	Telefone Encarregado
pedro.costa@g23.com	11-98855-5588

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 "Hamburgão da Galera Lanches" informa que, diante de sua atividade principal de venda de lanches, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

a) coleta e trata dados pessoais e sensíveis como nome, CPF e email, caso o titular queira fazer o cadastro e ter facilidade nos próximos pedidos. Os dados são armazenados e tratados para agilizar a venda e entrega do pedido.

b) trata dados pessoais do TITULAR, este identificado como cliente, no contexto do interesse legítimo do controlador em razão de sua responsabilidade na comunicação de dados fiscais às autoridades competentes.

c) trata 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 e/ou serviços prestados pela CONTROLADORA ao TITULAR.

Todos 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. A título exemplificativo, porém não exaustivo, segue link das principais que envolvem dados do TITULAR - http://www.escritoresassociados.com.br/obrigacoes_lgpd.htm

3.1.– TRATAMENTO

- Os dados são inseridos manualmente no sistema, salvos em banco de dados criptografado e armazenados por 5 anos ou até o titular pedir sua exclusão;
- Os dados são informados diretamente pelo Titular.
- Os dados não são compartilhados além do sistema e operadores.

4.– PARTES INTERESSADAS CONSULTADAS

1. Entidades legais consultadas

1. Erick Muller – Especialista em Engenharia de Software e análise de dados;
2. Ana Beatrice Braga – Professora e Advogada especialista em Proteção de Dados e LGPD

2. Encarregado dos dados, como citado na seção 1.
3. Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por Donald M., 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, 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

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R 01	Erro de operação pelo operador gerando dados errados	15	10	150
R 02	Acesso não autorizado	5	15	75
R 03	Falha do serviço em nuvem gerando indisponibilidade dos dados	5	10	50
R 04	Falha do serviço de banco de dados e perda deles	5	15	75
R 05	Falha no serviço de retenção mantendo os mesmos mais do que 5 anos	5	5	25
R 06	Compartilhar dados sem autorização	`5	15	75
R 07	Falha no serviço de remoção dos dados	5	10	50

Legenda: P – Probabilidade; I – Impacto.

7.– MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual			Medida(s) Aprovada(s)
			P	I	Nível (P x I)	

R01	Treinamento dos operadores; Supervisão da operação por operador Sênior; Validação dos dados entrados no sistema	Reduzir	5	5	25	Sim
R02	Controle de acesso físico; Controle de acesso lógico; Monitoramento por câmeras do ambiente;	Reduzir	5	5	25	Sim
R03	Utilizar serviços de alta disponibilidade; Acesso Internet backup; Testes de estresse do sistema	Reduzir	5	5	25	Sim
R04	Utilizar serviços de alta disponibilidade; Provedor de alta confiabilidade; backup recorrente	mitigar	5	0	0	Sim
R05	Teste e simulação no sistema	mitigar	0	0	0	Sim
R06	Treinamento dos operadores; Supervisão da operação por operador Sênior	Reduzir	5	5	25	Sim
R07	Testes de sistema; logs e notificações; automação para confirmar a remoção	mitigar	0	0	0	Sim

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

8.– APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO

_____ Pedro Costa	_____ Pedro Costa

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
_____ Josué Galera	_____ Ronald McDonald