RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 18 de março de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controladora: Lanchonete BOMLANCHE

Operador(es): João da Silva, Pedro Souza, Maria Quitéria

Encarregado: Escritório ACME

E-mail do Encarregado: (etelvina@acme.com.br)
Telefone: (11) 912345-6789

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 atendimento de pedidos de fast food através de um sistema de autoatendimento digital, esclarece que:

a) Coleta e trata dados pessoais e sensíveis relativos à documentação fiscal (CPF), e-mail e nome do TITULAR, quando for identificado como cliente, e quando este efetuar uma compra através do sistema de autoatendimento, para fins de identificar o cliente e efetuar a entrega correta.

b) Trata dados que podem causar danos patrimoniais ao TITULAR, quando este identificado como cliente, referente a cartão de crédito, para receber pagamentos relativos a produtos vendidos pela CONTROLADORA ao TITULAR.

Os dados do primeiro item são coletados e tratados no contexto da prestação de serviços e venda de produtos, com a finalidade de identificação unívoca do cliente TITULAR (CPF), bem como a possibilidade de entrar em contato com o cliente para informá-lo de assunto do interesse dele (e-mail), a saber, recuperação de senha. Além disso, a manutenção dos dados do TITULAR possibilita o acesso mais rápido e eficiente do mesmo ao sistema de autoatendimento, ou seja, gera comodidade para o cliente.

Os dados do segundo item (cartão de crédito) não são armazenados pelo sistema, sendo utilizados apenas no momento do pagamento do pedido de compra.

4 - PARTES INTERESSADAS CONSULTADAS

1. Entidades legais consultadas

    1. Escritório ACME, representado por Carlos Madureira, especialista em avaliação de segurança de dados pessoais no contexto da LGPD;

    2. Secretaria Estadual de Segurança de Dados.

2. Encarregado dos dados, como citado na seção 1.

3. Especialistas de segurança da CONTROLADORA, notadamente: Manuel Bastos; Edite Figueiredo; Camila Andrade.

4. Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por Ronaldo Silva, 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 da CONTROLADORA, elaborou 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 da CONTROLADORA é uma das fundamentações em razão da necessidade de prover acesso ao TITULAR permitindo o autoatendimento, bem como a realização da compra através de pagamento eletrônico.

Todos os dados de identificação do TITULAR coletados com essa finalidade são eliminados uma vez que ele solicite a remoção do cadastramento do sistema. Enquanto o TITULAR desejar permanecer com acesso ao sistema, o encarregado manterá todos os dados criptografados através do serviço AWS Cognito.

A entidade CONTROLADORA poderá, a pedido do TITULAR, descadastrar o seu usuário, removendo todos os dados de identificação da plataforma.

Os dados de pagamento são solicitados apenas durante o processo de pagamento e, uma vez recebendo a autorização da entidade pagadora, não são armazenados.

É importante constar que não há, por legislação, a retroatividade do processamento dos dados, em caso de remoção do cadastramento do usuário. 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).

Risco	Especificação do Risco	P	I	Nível de 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 operação dos dados	5	5	25

7 - MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida	Efeito sobre o risco	Medida aprovada
R01	1. Acesso à plataforma onde os dados dos usuários são guardados (Cognito) é protegido através de uso de autenticação multifator (MFA) , uso de sistema de autorização da AWS (roles) e uso de SSL/TLS para se comunicar com os recursos da Plataforma.	reduzir	sim
R02	1. Treinamento. 2. redução de dados para operação. 3. Configuração do registro em log das atividades.	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