RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 05 de agosto de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Grupo 14

Encarregado: Grupo 14

Operador(es): Davi Donadelli, Juliana Maijer, Rafael Roque e Thomaz Palmeira

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 – PARTES ENVOLVIDAS

- Departamento Jurídico:
    - O departamento jurídico colaborou revisando as conformidades legais e regulatórias, garantindo que todas as práticas de tratamento de dados estejam em conformidade com a LGPD.
- Equipe de TI:
    - A equipe de TI avaliou as medidas técnicas de segurança e recomendou a implementação de criptografia de ponta a ponta, criptografia de dados no banco de dados, implementação de redundância e outros detalhes técnicos.
- Equipe de negócio e marketing:
    - As equipes de negócio e marketing colaboraram indicando quais e onde os dados serão usados, trouxeram também tratativas para casos de incidentes trazendo métodos para abordar os clientes.

4 – FINALIDADE DO TRATAMENTO DE DADOS

- Cadastro de usuários no sistema: o cliente pode cadastrar-se pra interagir com o sistema.
- Identificação de clientes em pedidos: o cliente pode escolher se identificar durante a criação de um pedido e neste caso um dado seu será usado como identificador.

- BI para campanhas da empresa. No futuro, os dados de endereço do cliente serão usados para fazer campanhas promocionais direcionadas.
- Comunicação com clientes. Permitir envio de e-mails ou notificações para os usuários do sistema.

5 – BASE LEGAL PARA TRATAMENTO

- Consentimento: os dados serão tratados com o consentimento explicito dos clientes, que inclusive será o único responsável por cadastrá-los no sistema.
- Execução de contrato: tratamento necessário para execução do contrato com o titulas dos dados

6 – DESCRIÇÃO DOS DADOS COLETADOS

- Dados pessoais coletados
    - Nome: nome do cliente. Deverá ser usado para dirigir-se ao cliente durante interações com o mesmo.
    - CPF: número do documento de CPF do cliente. Utilizado para identificação do cliente nos pedidos.
    - Email: endereço de e-mail do cliente. Meio utilizado para comunicar-se com o cliente.
    - Telefone celular: número do telefone celular do cliente. Outro meio utilizado para comunicar-se com o cliente.
    - Endereço: objeto que representa o endereço residencial do cliente. E composto por:
        - Rua
        - Cidade
        - Número
        - CEP
        - Bairro

7 – IDENTIFICAÇÃO DOS RISCOS

Número	Especificação	Probabilidade	Impacto
R01	Acesso não autorizado	Alta	Médio
R02	Operação incorreta dos dados	Alta	Baixo
R03	Perca de dados	Média	Baixo
R04	Vazamento de dados	Baixa	Médio

8 – ANÁLISE DETALHADA DOS RISCOS E MEDIDAS DE MITIGAÇÃO

- **R01: Acesso não autorizado**
    - Descrição: a possibilidade de indivíduos não autorizados dentro da companhia acessarem dados pessoas dos clientes
    - Medidas de mitigação:
        - Limitar acesso a dados reais dos clientes por roles: criar roles para os colaboradores que limitem o acesso às informações dos clientes.
        - Criar ambiente de desenvolvimento com alteração dos dados reais: diferenciar ambientes de produção e desenvolvimento para que equipes de desenvolvimento e homologação do produto não acessem e interajam com dados reais dos clientes.
    - Risco ao usuário: pode ter dados sensíveis sendo acessados por terceiros.
- **R02: Operação incorreta dos dados**
    - Descrição: erros ou falhas de sistema que possam resultar em dados incorretos.
    - Medidas de mitigação:

        - Treinar pessoal para auxiliar clientes: operadores devem ser treinados para ajudar os clientes caso estejam presentes num incidente de falha do sistema.
        - Permitir edição de dados após cadastro: o sistema precisa dar a chance para o cliente editar seus dados após cadastro para corrigir possível erro do usuário.
        - Implementar camada de validação de dados do cadastro para evitar cadastro de informações incorretas: APIs precisam validar os dados cadastrados pelo cliente para evitar erros durante cadastro.
    - Risco ao usuário: pode afetar negativamente na experiência do usuário durante uso do sistema.

- **R03: Perca de dados**
    - Descrição: dados podem ser perdidos devido a falhas no sistema
    - Medidas de mitigação:
        - Utilizar base de redundância: deve-se ter uma base de redundância que deverá ser consultada para recadastramento de dados caso na base original ocorra falha que resulte em perca de dados.
    - Risco ao usuário: pode afetar negativamente na experiência do usuário durante uso do sistema.

- **R04: Vazamento de dados**
    - Descrição: dados sensíveis dos clientes podem ser expostos indevidamente a terceiros
    - Medidas para mitigação:
        - Salvar informações criptografadas: usar criptografia para proteger os dados para evitar exposição dos mesmos caso o banco seja invadido.
        - Reduzir quantidade de dados transferido nas APIs: criar APIs que transportem a menor quantidade possível de dados para mitigar ao máximo o vazamento caso haja alguma invasão à essa comunicação.
        - Implementar política de segurança de acesso aos dados: proteger credenciais que permitem acesso a banco de dados do sistema.

- Risco ao usuário: pode ter dados sendo vazados para terceiros que podem fazer uso nocivo desses dados e afetar negativamente o usuário.

9 – PLANO DE AÇÃO EM CASO DE INCIDENTES

- Comunicação aos titulares: conversar com os donos dos dados a fim de informar sobre os dados afetados.
- Auditoria interna: entender o que aconteceu para identificar a causa do incidente e implementar medidas corretivas
- Revisão do processo de segurança: revisar e aprimorar documentação, processos e sistemas de segurança para evitar futuros incidentes
- Treinamento da equipe para melhorar atendimento aos incidentes

10 – INATIVAÇÃO DOS DADOS PESSOAIS

O sistema possui uma API que possibilita aos usuários solicitar a inativação de seus dados pessoais no sistema. Essa função visa garantir o direito do usuário de requisitar a interrupção do uso de suas informações pelo sistema.