Política de Segurança da Informação e Privacidade

Omie.Store

Índice

1. Introdução

Esta política tem como objetivo principal estabelecer diretrizes de **Segurança da Informação e Privacidade** para os parceiros da OMIE.STORE, a fim de garantir a proteção dos dados e informações confidenciais da Omie e de nossos Clientes.

Para fins dessa política, informações confidenciais são consideradas:

- Dados pessoais e dados pessoais sensíveis
- Dados financeiros
- Dados de cartão de crédito

2. Abrangência

Todas as empresas que oferecem produtos na OMIE.STORE.

3. Disposições Iniciais

3.1. Segurança da Informação

A Segurança da Informação é caracterizada pela proteção dos dados e informações de ameaças internas e externas, garantindo a preservação dos seguintes princípios:

Confidencialidade – garantia de que a informação é acessível somente por pessoas com acesso autorizado;

Integridade – é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

Disponibilidade – garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

É considerado incidente de segurança da informação o descumprimento desta política, bem como qualquer violação de dados (violação de segurança que leva à destruição acidental ou ilícita, perda e divulgação não autorizada de dados, acesso não autorizado).

3.2. Privacidade

O tratamento de dados pessoais deve garantir a privacidade dos dados de pessoas físicas conforme descrito na LGPD (Lei Geral de Proteção de Dados). Para isso considera-se:

DADO PESSOAL: qualquer informação relacionada a uma pessoa física identificada ou identificável, portanto todo aquele dado que identifique uma pessoa física, ou que, por meio de um conjunto de dados, possa vir a identificar uma pessoa física, por exemplo: nome, RG, CPF, endereço, dados de acesso à internet, telefone, e-mail etc.

TITULAR DO DADO: pessoa física a quem os Dados Pessoais são objeto do Tratamento

4. Diretrizes

4.1. Diretrizes Gerais

- Todos os parceiros serão avaliados quanto à saúde cibernética antes do ingresso na Omie.Store.
- Os parceiros serão monitorados durante a permanência do seu aplicativo na Omie.Store.
- A Omie se reserva no direito de realizar análises e auditorias de segurança e privacidade para garantir a proteção de suas informações e de seus clientes.

4.1.1. Avaliação para entrada na Omie.Store

- Os parceiros serão avaliados pela Omie, antes da assinatura do contrato, no que tange à segurança cibernética através de uma plataforma que provê uma pontuação (A, B, C, D e F), onde **A** é a pontuação máxima.
- Após a avaliação, o parceiro receberá um relatório e deverá providenciar o tratamento das vulnerabilidades nele contidas.
- Para ingressar na Omie.Store, o parceiro deverá obter a pontuação **A** e não possuir vulnerabilidades altas.
- Caso o parceiro tenha uma pontuação abaixo do permitido, ele deverá tratar as vulnerabilidades apontadas no relatório, com o objetivo de atingir a pontuação **A**.
- Adicionalmente, todos os parceiros deverão responder a um formulário com o objetivo de identificar sua conformidade quanto às diretrizes da Política de Segurança da Informação da Omie.
- As respostas serão avaliadas quanto à conformidade com essa política de segurança, de acordo com o tipo de serviço e a sensibilidade dos dados tratados.

- O parceiro deve manter o ambiente do Aplicativo ofertado na Omie.Store livre de ameaças, sendo de sua responsabilidade a identificação e correção de vulnerabilidades que comprometam a segurança das informações da Omie e de seus Clientes.
- As informações confidenciais tratadas no sistema/aplicativo devem ser protegidas contra acesso, modificação, destruição ou divulgação não autorizada de forma a manter a Confidencialidade e Integridade.

4.1.2. Monitoramento

- Durante a vigência do contrato, os parceiros serão monitorados pela Omie a fim de que mantenha a pontuação **A** exigida para operação.
- O parceiro deverá manter a pontuação **A** durante a permanência do aplicativo na Omie.Store.

4.2. Diretrizes de Segurança da Informação

Governança de Segurança e Privacidade

- Os colaboradores do parceiro devem ser orientados e conscientizados sobre a Política de Segurança da Informação e Privacidade da Omie.Store;
- O parceiro deve manter uma Política de Segurança da Informação e Privacidade atualizada;

Ambiente de Processamento e Armazenamento de dados

O ambiente de processamento e/ou armazenamento de dados e informações deve ser:

- Protegido contra códigos maliciosos;
- Protegido contra ameaças cibernéticas;
- Sempre atualizado;
- Avaliado constantemente a fim de identificar vulnerabilidades e realizar as devidas correções.

Uso de Criptografia

- As informações confidenciais devem ser criptografadas em trânsito e em repouso;

Controle de Acesso

O sistema/aplicativo deve possuir controles relacionados ao login como:

- Uso de senhas complexas;

- Forçar alteração de senha no primeiro acesso;
- Bloquear acesso após determinadas tentativas inválidas;
- Uso de autenticação de múltiplo fator para informações confidenciais.

Segurança no desenvolvimento de sistemas

- O parceiro deve desenvolver seus sistemas e aplicativos de acordo os padrões de segurança e privacidade aceitos pelo mercado e em conformidade com a LGPD (Lei Geral de Proteção de Dados).
- A diretriz de *Security and Privacy by default* deve ser observada no desenvolvimento de sua aplicação.
- O parceiro deve realizar validações de segurança onde devem ser consideradas no mínimo aquelas que constam na metodologia OWASP TOP 10.
- O parceiro deve realizar testes de intrusão anualmente para garantir a segurança da aplicação.

Continuidade do negócio

- O sistema/aplicativo deve manter um plano que garanta a sua continuidade em caso de algum incidente que afete a sua disponibilidade;
- O parceiro deve manter uma rotina de testes a fim de garantir a efetividade do plano de continuidade do negócio.

4.3. Diretrizes para o Tratamento de dados pessoais

- O tratamento de dados pessoais deve ser realizado em conformidade com a Lei Geral de Proteção de Dados (LGPD).
- O parceiro deve possuir Política de Privacidade com as informações pertinentes para dar transparência ao tratamento de dados pessoais no sistema/aplicativo disponibilizado na Omie.Store.
- O parceiro deve manter uma análise de impacto relacionada aos dados pessoais (DPIA), a fim de identificar os riscos relacionados ao tratamento de dados pessoais.
- O parceiro deve observar a Política de Privacidade da Omie.

5. Uso de APIs

As APIs para integração com o Sistema de Gestão OMIE estão disponíveis no Portal do Desenvolvedor (https://developer.omie.com.br/).

6. Subcontratação de Serviços

- O parceiro que optar pela subcontratação de parte ou todo o escopo de serviços deve manter explícita a finalidade do compartilhamento de dados em suas políticas de privacidade e segurança, indicando nos mesmos instrumentos quais dados serão compartilhados.
- É de responsabilidade do parceiro a garantia do cumprimento das diretrizes aqui dispostas pelo subcontratado.

7. Notificação de Incidentes

- Os incidentes de segurança da informação e privacidade envolvendo dados pessoais e informações da Omie e de seus clientes devem ser comunicados em até 24 horas contadas do conhecimento ou mera suspeita do incidente.
- As suspeitas e/ou incidentes de segurança da informação devem ser informados através do e-mail ciso@omie.com.br.
- As suspeitas e/ou incidentes de segurança envolvendo o tratamento de dados pessoais devem ser informados através do e-mail privacidade@omie.com.br.

8. Revisões

Esta política será revisada quando houver mudanças nas diretrizes.