Cartilha de Boas Práticas de Proteção de Dados Pessoais para Fornecedores

1. Introdução

Propósito:
A proteção de dados pessoais é uma prioridade global, com regulamentações específicas em diversos países que buscam garantir os direitos dos titulares. Além da Lei Geral de Proteção de Dados (LGPD) no Brasil, a Dock também está sujeita a legislações de outros países, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, a Lei de Proteção de Dados Pessoais do México, entre outras. Esta cartilha estabelece padrões para que fornecedores e parceiros possam assegurar a conformidade com todas as normas aplicáveis.

A Importância para a Dock:
Para a Dock, que lida com dados pessoais e sensíveis em mercados internacionais, garantir a segurança e a privacidade é essencial para construir confiança e manter a integridade das operações. Assim, espera-se que todos os fornecedores alinhem suas práticas às legislações de privacidade aplicáveis em cada país onde atuam, promovendo um ambiente de negócios responsável e ético.

---

2. Definição de Dados Pessoais

Dado Pessoal:
Dados pessoais são informações relacionadas a uma pessoa identificada ou identificável, conforme definições legais de cada jurisdição. Exemplos incluem nome, CPF, endereço, telefone, e-mail e informações financeiras.

Dado Pessoal Sensível:
São dados que exigem proteção adicional devido ao seu potencial de causar discriminação ou prejuízo, como informações biométricas, de saúde, orientação sexual ou convicções religiosas.

---

3. Princípios Globais de Proteção de Dados

Embora haja variações entre legislações, os seguintes princípios são amplamente reconhecidos:

- **Finalidade:** Os dados devem ser tratados apenas para objetivos legítimos e claros.
- **Minimização de Dados:** Coletar apenas o necessário para a finalidade declarada.
- **Transparência:** Informar claramente como os dados são tratados.
- **Segurança:** Implementar medidas adequadas para proteger os dados contra acessos não autorizados e perdas.
- **Responsabilização:** Demonstrar conformidade com as normas aplicáveis por meio de documentação e práticas adequadas.

---

4. Obrigações dos Fornecedores

1. **Conformidade Multijurisdicional:** Identificar e cumprir as legislações aplicáveis no tratamento de dados pessoais, considerando os locais de operação.
2. **Proteção de Dados por Design:** Adotar práticas que integram a proteção de dados desde o início de processos e projetos.
3. **Subcontratação:** Informar previamente à Dock sobre subcontratados envolvidos no tratamento de dados e assegurar que também estejam em conformidade.

---

5. Direitos dos Titulares

Os direitos variam conforme a legislação, mas incluem:

- **Acesso, Retificação e Portabilidade:** Solicitação de acesso, correção e transferência de dados pessoais.
- **Eliminação:** Atender a solicitações de exclusão de dados, salvo exceções legais.
- **Restrição ou Oposição ao Tratamento:** Possibilidade de restringir ou se opor ao uso de dados em casos específicos.

---

6. Medidas de Segurança

- **Criptografia e Controle de Acesso:** Proteger dados em trânsito e em repouso.
- **Monitoramento e Prevenção de Incidentes:** Realizar auditorias e treinar equipes para identificar e responder rapidamente a riscos de segurança.
- **Relato de Incidentes:** Notificar imediatamente a Dock sobre qualquer incidente que envolva dados pessoais.

---

7. Transferência Internacional de Dados

Garantir que a transferência de dados para outros países ocorra conforme os requisitos legais, incluindo:

- **Bases Legais para Transferência:** Como cláusulas contratuais padrão, consentimento ou adequação do país receptor.
- **Monitoramento e Auditoria:** Manter registros das transferências realizadas e revisar práticas dos países receptores.

---

8. Governança e Conformidade

1. **Auditorias e Avaliações:** Permitir inspeções pela Dock para verificar a conformidade.
2. **Programas de Treinamento:** Promover educação contínua sobre proteção de dados para equipes e parceiros.
3. **Relatórios Regulares:** Fornecer evidências periódicas de conformidade.

---

9. Consequências em Caso de Não Conformidade

A não conformidade pode resultar em:

- Multas e penalidades administrativas impostas por autoridades reguladoras.
- Rescisão de contratos e exclusão do rol de fornecedores da Dock.
- Danos reputacionais e comerciais, afetando todas as partes envolvidas.

---

10. Contato e Comunicação

Canal de Comunicação Direto: Dúvidas, incidentes ou solicitações relacionadas à proteção de dados pessoais devem ser comunicados por meio do nosso **portal de privacidade**: https://dock.tech/privacidade/.

Nota Final:
A conformidade é um esforço contínuo. Esteja sempre atento às mudanças regulatórias e mantenha-se atualizado para proteger os dados pessoais de forma eficaz.