Fluxo de Avaliação de Privacidade em Fornecedores

1. PROSPECÇÃO

Checkpoint: Validação pública

2. RFI (Request For Information)

Checkpoint: Evidências técnicas

3. ANÁLISE

Checkpoint: Avaliação de risco

4. NEGOCIAÇÃO

Checkpoint: Cláusulas de privacidade

5. ASSINATURA

Checkpoint: Contrato aprovado

Este fluxo detalha as etapas cruciais para a avaliação de privacidade de fornecedores, com foco nos checkpoints críticos para garantir a conformidade e mitigar riscos. Cada etapa é fundamental para assegurar que os parceiros de negócio estejam alinhados com as políticas de privacidade da empresa.

Matriz de Risco: Requisitos de Privacidade por Categoria de Fornecedor

Esta matriz ajuda a classificar os fornecedores com base no nível de risco de privacidade e define os requisitos mínimos e certificações necessárias para cada categoria.

NÍVEL DE RISCO	EXEMPLOS DE SOFTWARE	CERTIFICAÇÕES OBRIGATÓRIAS	REQUISITOS MÍNIMOS
ALTO RISCO	CRM (Salesforce), HRM (Workday), Sistemas Financeiros, Processamento de Pagamentos	ISO 27001, SOC 2 Type II, ISO 27701 (desejável)	RFI detalhada obrigatória, Auditoria anual, DPO nomeado, Cláusulas completas, Direito de auditoria surpresa
MÉDIO RISCO	Colaboração (Slack), Analytics (Mixpanel), Marketing (Mailchimp), Project Management	ISO 27001 OU SOC 2	RFI simplificada, Revisão documental anual, Cláusulas prioritárias, Notificação de incidentes, Controle de subprocessadores
BAIXO RISCO	Ferramentas internas, Utilitários sem dados sensíveis, Design/ Prototipagem, Produtividade básica	ISO 27001 (desejável), Certificações não obrigatórias	Validação pública suficiente, Cláusulas básicas, Confidencialidade, Limitação de uso, Auditoria não obrigatória

Dica: *A classificação de risco de um fornecedor deve sempre considerar o tipo de dados processados, o volume de dados e a criticidade dos serviços para o negócio.*

Checklist Essencial: O que incluir em sua RFI de Privacidade

RFI de Privacidade - Request for Information - Modelo Completo

1

- ○ Quem é o DPO ou responsável pela privacidade?
- ○ Como a empresa gerencia riscos de privacidade?
- ○ Existe comitê de privacidade ou governança formal?
- ○ Qual a estrutura organizacional de proteção de dados?

2

- ○ Possui ISO 27001 ou SOC 2 Type II vigentes?
- ○ Quando foi a última auditoria externa?
- ○ Fornece cópias atualizadas dos certificados?
- ○ Possui ISO 27701 ou certificações específicas de privacidade?

3

- ○ Onde os dados serão armazenados (país, região)?
- ○ Qual a arquitetura de rede e controles de acesso?
- ○ Utiliza criptografia (TLS 1.2+, AES-256)?
- ○ Possui autenticação multifator (MFA)?
- ○ Quais subprocessadores/subcontratados são utilizados?

4

- ○ Qual o processo de notificação de incidentes?
- ○ SLA para notificação (idealmente < 72h)?
- ○ Houve incidentes de segurança nos últimos 24 meses?
- ○ Possui seguro de responsabilidade cibernética?

Dica: *Adapte este checklist e seus requisitos com base no nível de risco do fornecedor e na sensibilidade dos dados processados.*