



Procedimento de Avaliação de Conformidade LGPD de Fornecedores e Parceiros

VendeAI Tecnologia

POL-VDA-11 — versão 1.0

1 Introdução

Este procedimento estabelece os critérios que a VendeAI Tecnologia (“VendeAI”) deve observar para avaliar a conformidade com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD), de fornecedores e parceiros que tratem dados pessoais em nome da empresa ou tenham acesso a esses dados no âmbito de uma relação contratual.

2 Objetivo

Garantir que a VendeAI contrate e mantenha relações apenas com fornecedores e parceiros que demonstrem nível adequado de maturidade em proteção de dados pessoais e segurança da informação, mitigando o risco de incidentes decorrentes de terceiros.

3 Escopo

Aplica-se a toda contratação de fornecedor, parceiro comercial, prestador de serviço ou instituição financeira que envolva tratamento, acesso ou armazenamento de dados pessoais de clientes, colaboradores ou parceiros da VendeAI.

4 Referência documental

Este procedimento observa, entre outras normas aplicáveis:

- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD);
- Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);
- Cláusula Padrão de Proteção de Dados Pessoais da VendeAI (POL-VDA-10).

5 Critérios de avaliação

Antes da contratação (ou, no mínimo, previamente à disponibilização de dados pessoais ao terceiro), a VendeAI avalia:

- existência de política de privacidade e/ou política de segurança da informação do fornecedor;
- existência de Encarregado de Proteção de Dados (DPO) ou responsável equivalente;
- histórico de incidentes de segurança relevantes conhecidos publicamente;
- medidas de segurança técnica declaradas (criptografia, controle de acesso, backups);
- inclusão da **Cláusula Padrão de Proteção de Dados Pessoais** (POL-VDA-10) no contrato firmado;
- localização do armazenamento dos dados (Brasil ou exterior) e eventuais salvaguardas para transferência internacional, quando aplicável.

6 Processo

1. A área responsável pela contratação preenche um checklist de due diligence LGPD, com apoio do DPO, antes de formalizar a contratação de fornecedor/parceiro que tratará dados pessoais;
2. O DPO revisa o checklist e, quando necessário, solicita documentação complementar ao fornecedor/parceiro (política de privacidade, evidências de segurança);
3. A contratação só é formalizada com a inclusão da cláusula padrão de proteção de dados no contrato;

4. Fornecedores e parceiros já contratados são reavaliados periodicamente (recomendado: anualmente), ou sempre que houver indício de não conformidade ou incidente de segurança envolvendo o terceiro.

7 Não conformidade

Fornecedores e parceiros que não atendam aos critérios mínimos desta avaliação, ou que se recusem a fornecer documentação/evidências solicitadas, não devem receber acesso a dados pessoais tratados pela VendeAI até a regularização da pendência. Em caso de não conformidade grave ou incidente de segurança relevante causado pelo terceiro, a relação contratual deve ser reavaliada pela liderança da VendeAI, podendo ser encerrada.

8 Responsáveis

Papel	Responsável
Autor	Gustavo Schewinski — CTO e DPO
Responsável da área	Gustavo Schewinski — CTO e DPO
Aprovador	Nicolas Ignacio Ryberg — CEO

9 Divulgação

Este procedimento é de uso interno, disponibilizado às áreas comercial e técnica da VendeAI responsáveis pela contratação de fornecedores e parceiros.