

AI and Automation Policy

Use automation while retaining control, privacy and responsibility.

Key points for reference

- Automation must respect limits and authorization.
- Do not send secrets to external models.
- Generated outputs need human review.

Reference summary. The complete clauses below prevail.

1. Scope

This governs AI and automation in Zovvi services and purchased customer resources. It does not assert that all support uses AI, a specific tool is active or Zovvi builds models. Offers must disclose included automated features and relevant limitations.

2. Data and confidentiality

Do not submit secrets, full banking data, databases or confidential content to external models without grounds, authorization and safeguards. APIs do not remove privacy, transfer or provider-contract requirements.

Hosting does not grant general permission to train AI on customer content. Additional Zovvi uses need purpose, legal grounds, disclosure and authorization where required, rather than presumed purchase consent.

3. Prohibited uses and rights

Fraud, phishing, unlawful social engineering, unauthorized exploitation, spam, unlawful discrimination and rights violations are prohibited. Synthetic voice, likeness and content must respect personality rights, authorization and required labeling.

Check model, input and output licenses. Generation does not prove originality or ownership; Zovvi cannot grant third-party rights.

4. Oversight and sensitive decisions

Check facts, security and suitability before publishing or executing generated code. Automated guidance may err and does not replace professional legal, medical or financial analysis. Deleting data or changing DNS or access needs authorization and review.

Solely automated decisions affecting individuals must respect LGPD transparency and review rights. Requests go to ola@zovvi.com.br; automated correctness is not guaranteed.

5. Usage, bots and integrations

Bots and agents must respect authentication, plan limits, APIs, disclosed quotas and target rights. Do not evade limits using multiple accounts, abusive IP rotation or distributed execution. Intensive workloads incompatible with shared hosting need an appropriate product.

Vague agent instructions do not authorize extraordinary costs. Keys need minimal scope and defined limits. Capacity increases and extras require disclosed prices and acceptance.

6. Incidents and enforcement

Abuse may be contained under the AUP with evidence, proportionality and review. Report dangerous outputs or exposure through official channels without repeating attacks or publishing secrets. Material purpose, provider or data-use changes require transparency and appropriate legal and contractual measures.

