AI & POPIA

What South African businesses need to know

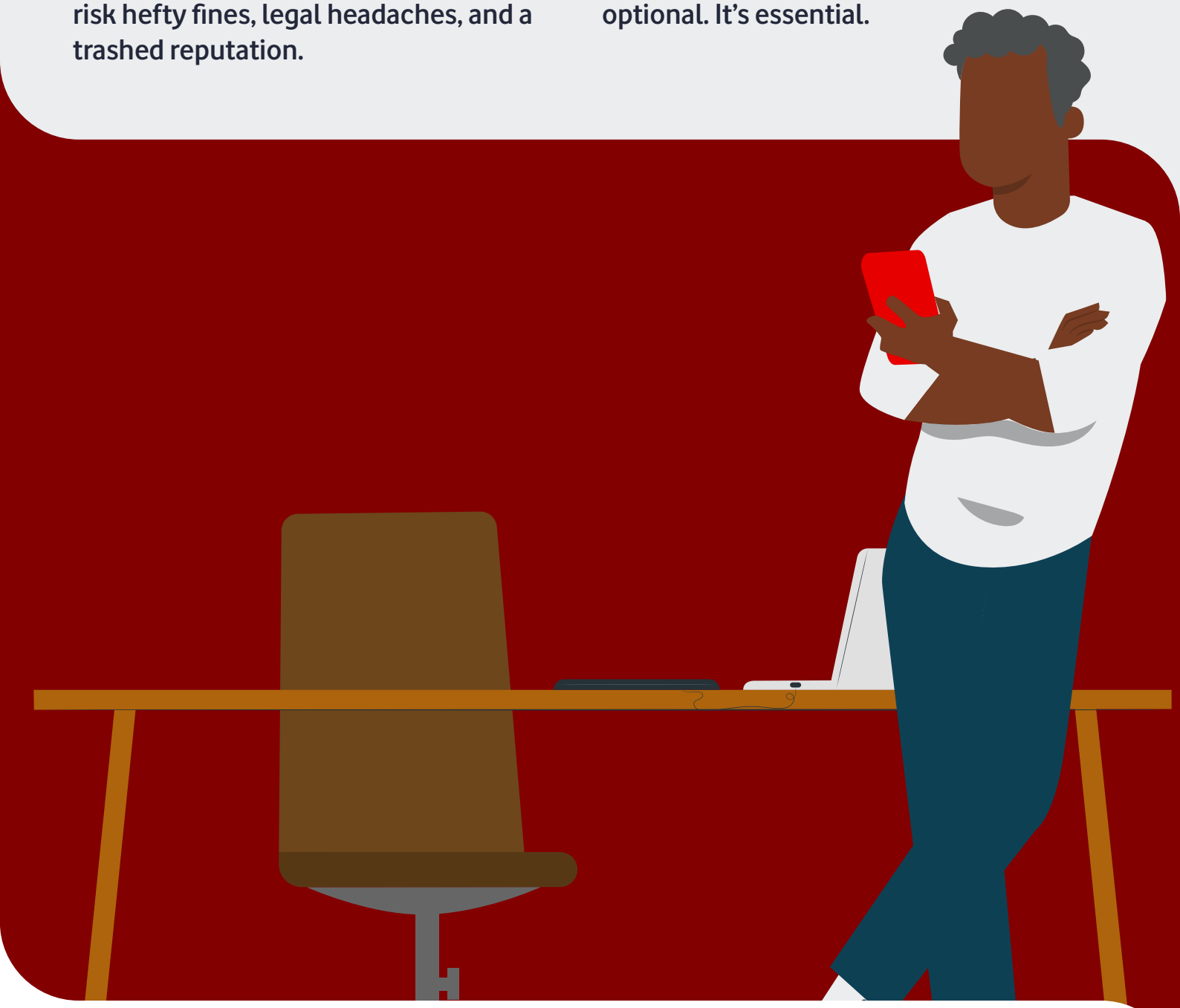
vodacom business

Introduction

AI tools are game-changers for businesses—unlocking creativity, efficiency, and growth like never before. But there's a catch: with great power comes legal responsibility.

That's where the Protection of Personal Information Act (POPIA) comes in to keep personal data in check. Ignore it, and you risk hefty fines, legal headaches, and a trashed reputation.

Whether you're experimenting with AI or already integrating it into your workflows, understanding the compliance side isn't optional. It's essential.



vodacom business

The POPIA principles that matter most for AI

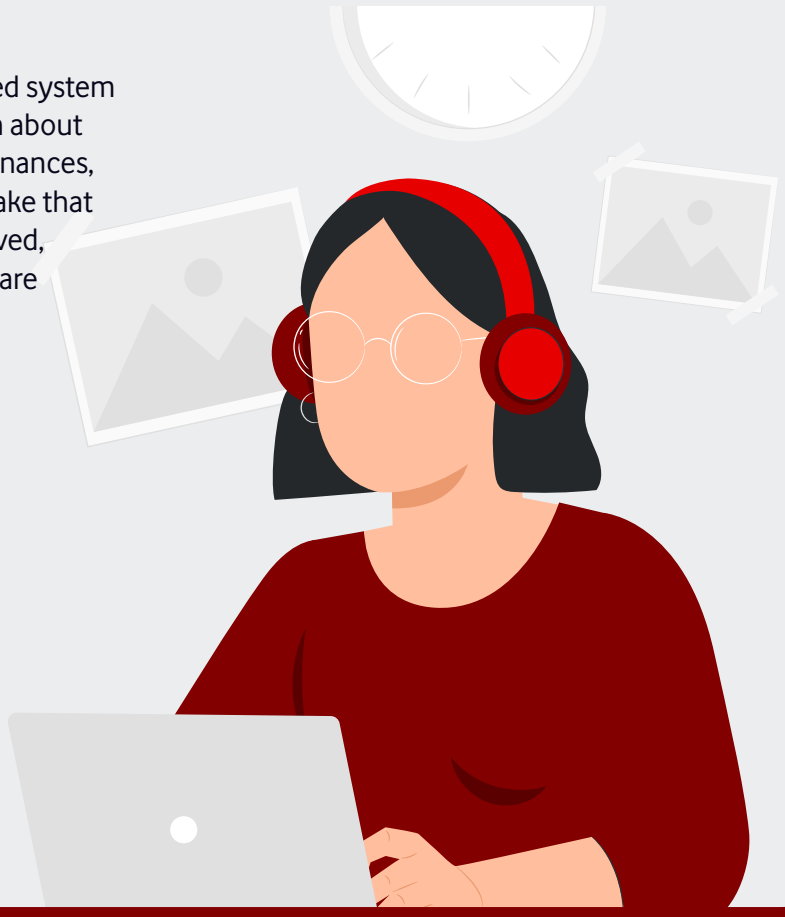
POPIA has eight core principles, but when it comes to AI, these stand out:

1. Data and purpose minimisation

Sections 10 and 13 of POPIA state you can only collect the data you truly need (Section 10), and you must use it only for the reason it was collected (Section 13). When using AI tools, this means avoiding bulk uploads of personal data that go beyond the task at hand, and making sure your AI use doesn't drift from the purpose the data was collected for. If the data was gathered for customer support, for example, using it in AI workflows is fine—as long as that use is consistent with the original intent and reasonably expected by the person involved.

2. Human oversight

Section 71 of POPIA states that if an automated system (like an AI tool) is going to make a big decision about someone—something that affects their job, finances, or opportunities—you can't let the system make that call on its own. There has to be a human involved, unless it's something required by law or there are strong protections in place to make sure the person is treated fairly and their rights are respected. Businesses must not only monitor AI outcomes but also ensure a person reviews and validates them. This helps avoid bias, ensures fairness, and meets the legal requirement for accountability in automated decision-making.



vodacom business

The POPIA principles that matter most for AI

(Continued)

3. Security & accountability

Section 19 requires that responsible parties put in place reasonable technical and organisational measures to prevent the loss, damage, unauthorised destruction or unlawful access to personal information.

When it comes to AI, this means businesses must make sure the tools and systems they use for handling personal info are locked down tight. Things like encryption, limiting who can access the data, and storing it securely are a must. You also need records to show you're following the rules.

It's also important to know where your data is heading. A lot of AI tools process what you give them on servers all over the world. If that's happening, POPIA says you have to confirm those places have adequate data protection. Take a close look at the tool's privacy policy and terms: are they keeping your data? Sharing it? Using it to tweak their AI? If you don't get clear answers, you could be putting personal info at risk in places you can't control or that don't fit your compliance setup.

vodacom business

What to know about your AI

Before integrating any AI tool into your workflow, it's important to ask the right questions to ensure compliance and transparency. Use this to evaluate AI platforms you use:

1. Where is data processed and stored?

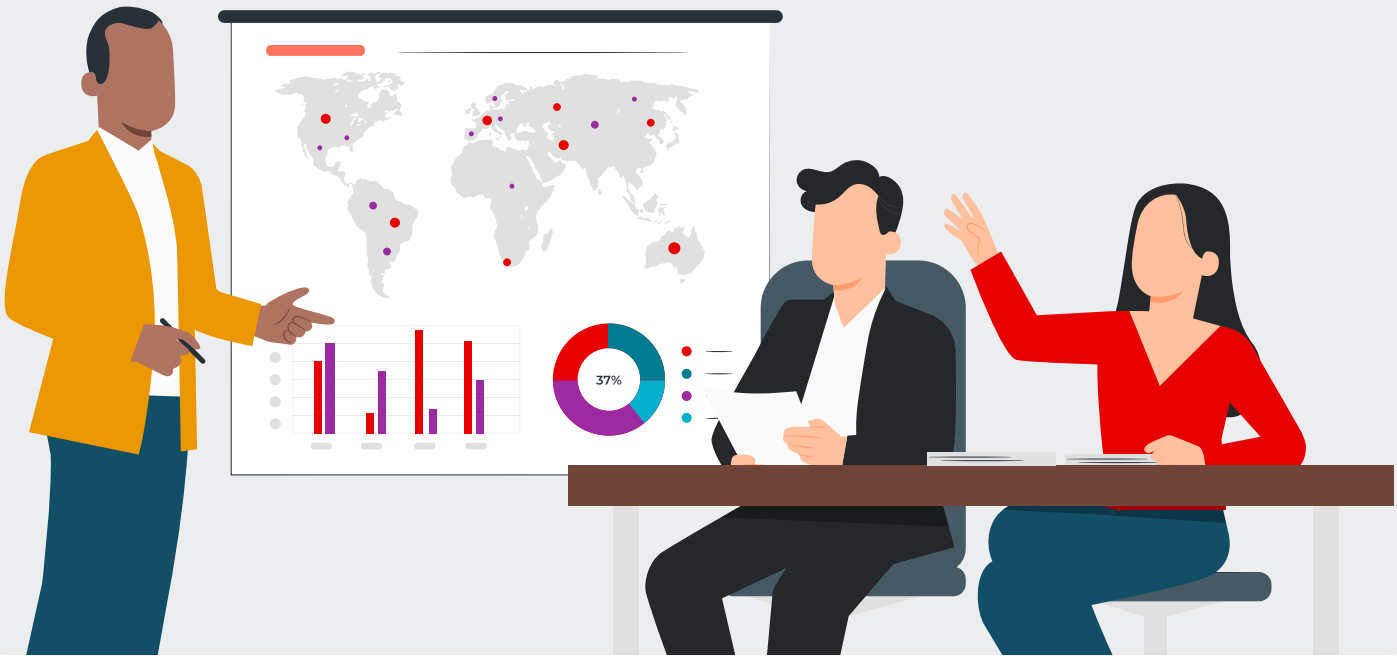
Make sure you understand if data is being transferred internationally, and whether it's stored in secure, POPIA-compliant environments.

2. Do they train the models using customer inputs?

Some AI tools learn from user input. If that's the case, your data could be retained and used to improve the tool for others. This may raise compliance concerns under POPIA—especially if the data includes personal information and is used in ways that go beyond the original purpose or is transferred to countries without adequate data protection. Make sure the AI practices align with your legal obligations and internal data handling policies.

3. Can you disable data logging or sharing features?

Ensure the tool allows you to opt out of data collection or usage logging where needed. The ability to turn off data sharing is key for sensitive workflows.



vodacom business

What to know about your AI

(Continued)

4. Do they offer logs or reporting features for compliance?

Ask whether the tool gives access to detailed activity logs, audit trails, or usage reports. These are essential for proving compliance in the event of an investigation.

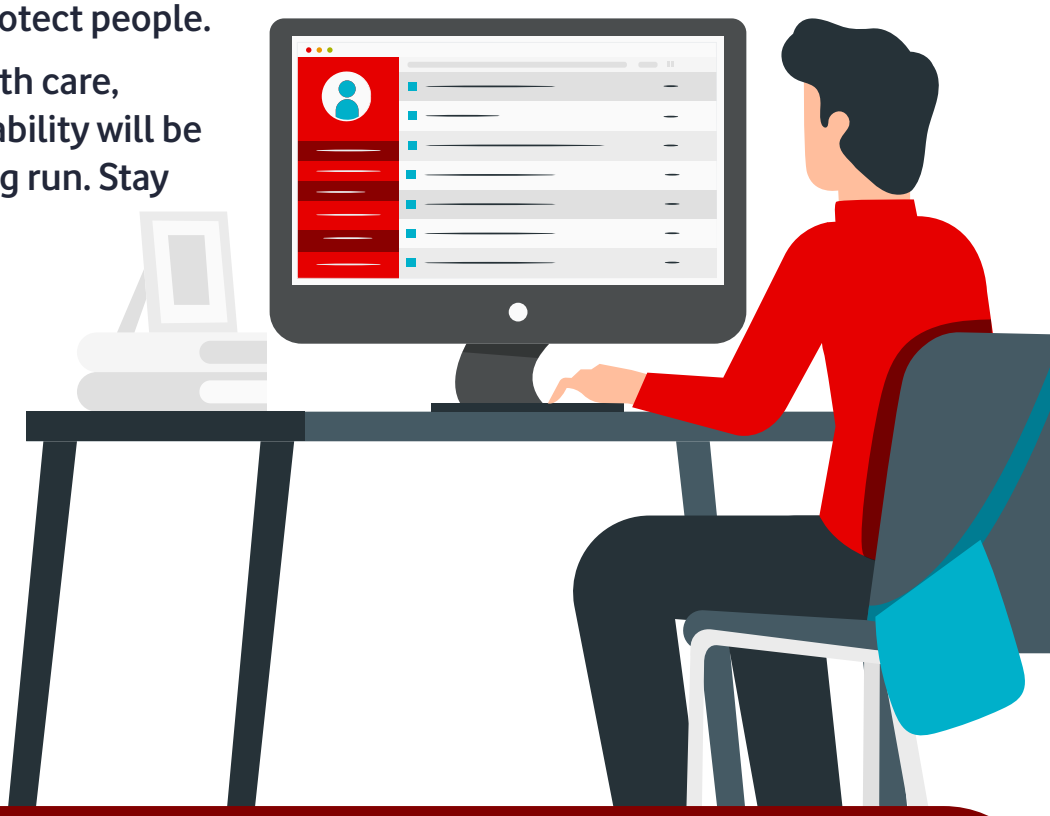
5. What security certifications or compliance standards do they meet?

Look for vendors that align with international data protection standards (like Microsoft Copilot) and can prove it.

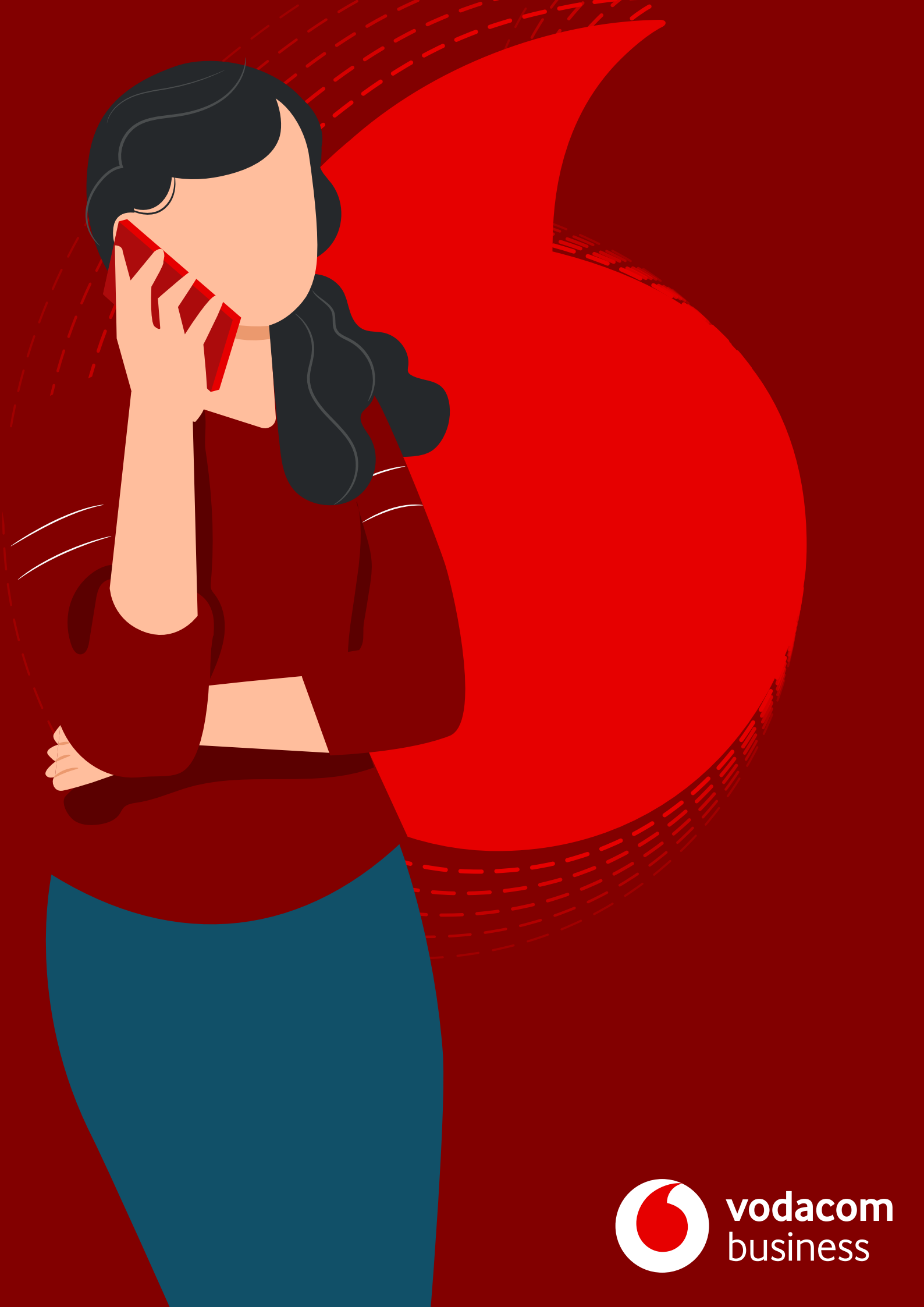
Conclusion

Using AI responsibly isn't just about avoiding fines. It's about building trust with your customers, employees, and partners. POPIA isn't there to block innovation—it's there to protect people.

Businesses that adopt AI with care, transparency, and accountability will be the ones that win in the long run. Stay smart. Stay compliant.



vodacom business


vodacom
business