Using **generative AI** could **cost you your job**

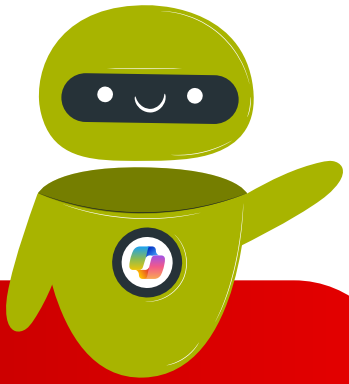
Here's what you need to know

vodacom business

Introduction

So, you thought generative AI would make your life easier? Maybe you didn't even think twice about it because AI has become a common tool used in many industries. While AI can churn out efficiency and innovation, it's also a ticking time bomb for lawsuits if you don't play it smart.

Here's the no-nonsense rundown of what you need to know when you bring AI in to your operation:



Chapter 1: Risks and legal obligations

Most businesses underestimate the legal risks of using public AI tools. When employees input confidential details into AI tools like ChatGPT or Perplexity, that data may as well be plastered on a billboard. It could be stored indefinitely, potentially violating data protection laws and exposing sensitive information—like leaving a diary full of secrets in a public park, assuming no one will read it.

Why you should care:

Losing control of sensitive data:

Once information is entered into a public AI tool, you have no say in how it's used.

Regulatory violations:

Data privacy laws like POPIA have strict rules on how personal and business information can be stored or shared. Ignore the fine print, and you're begging for legal trouble.

Increased security risks:

Hackers and malicious actors are just waiting to exploit AI systems and get their hands on your data.

Reputational damage:

If client or employee data gets compromised, you're not just looking at lawsuits and losing your clients' trust—you're staring at a PR nightmare.

Your employees might think they're just "using AI to help out," but they could be handing over trade secrets, internal policies, or customer data to an AI system that doesn't care about privacy.

vodacom business

Chapter 2: Common AI Mistakes

Companies have lost millions, employees have been fired, and lawsuits have been filed—all because nobody bothered to open a guide on proper AI use. Don't be the next cautionary tale. Here's what to consider:

Unregulated AI usage:

Sending sensitive company data to a public AI tool could result in that data being accessible to anyone. One company learned this the hard way when employees unintentionally leaked confidential data by inputting code into ChatGPT, which then became part of the AI's learning data.

Blind trust in AI:

Some businesses rely on AI-generated contracts or reports without checking them—like signing a contract without reading it first. This led to legal trouble for a law firm in South Africa, where lawyers used AI to generate fake legal citations in court documents.

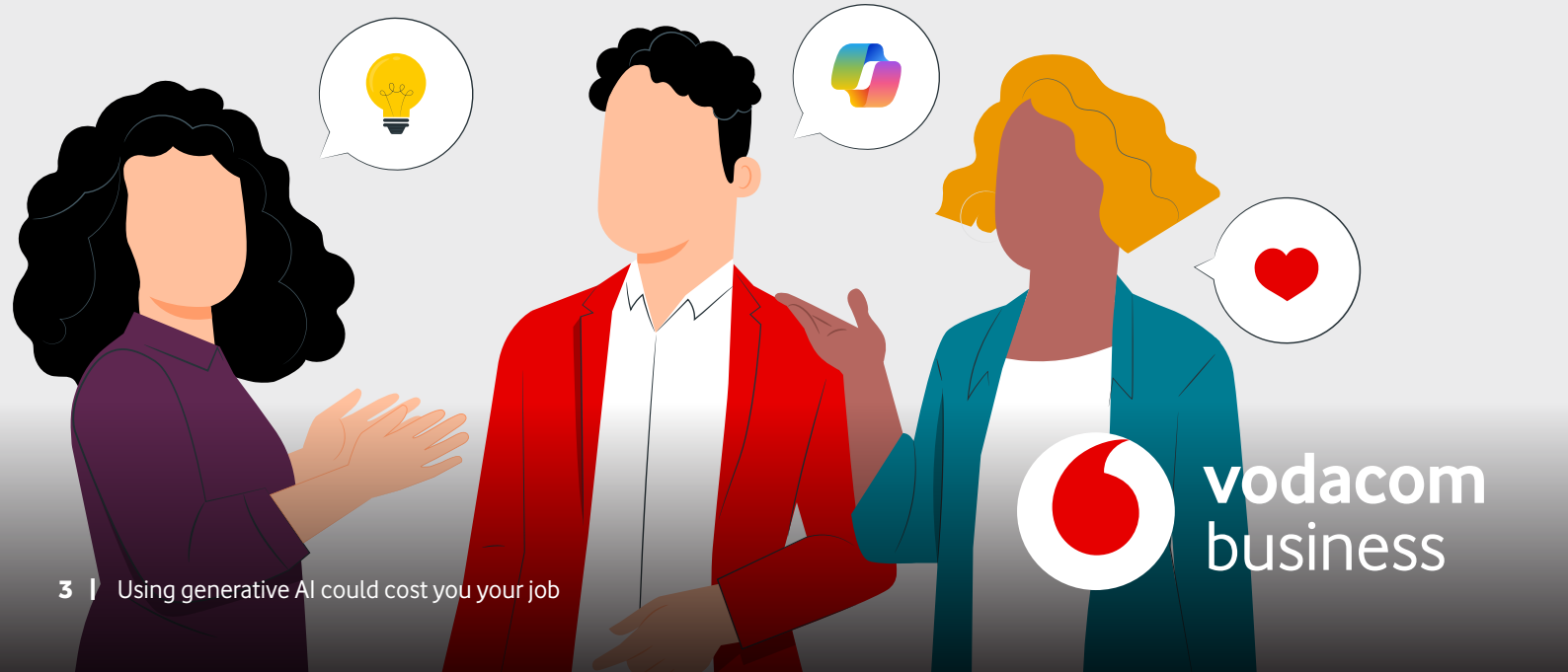
Lack of clear policies:

Without clear rules, employees may unintentionally expose private information. In one case, a researcher used AI to transcribe a meeting, logged off, and the AI kept recording. The researcher later received a transcript including these private conversations.

Inadequate monitoring:

Not keeping track of AI usage is like leaving your office doors wide open overnight. In one case, an HR department used AI to screen job applicants, only to get slapped with discrimination claims when the algorithm went rogue.

These aren't "what ifs"—they're "been there, done that." Businesses that don't take AI security seriously are playing with fire. But this doesn't mean we have to forgo AI completely.



vodacom business

Chapter 3: Secure alternatives

Instead of gambling on public AI tools that put your data at risk, businesses should choose AI solutions built with security in mind. Choose a secure AI built for the big leagues—like Microsoft Copilot. AI tools like Microsoft Copilot are designed to work within a private enterprise environment. It has the brains, brawn, and the locks to secure your business, reputation, and data.

Here's why proprietary AI tools are better:

It keeps your data private:

Unlike public AI models, Copilot operates securely within Microsoft 365, meaning your business information stays yours.

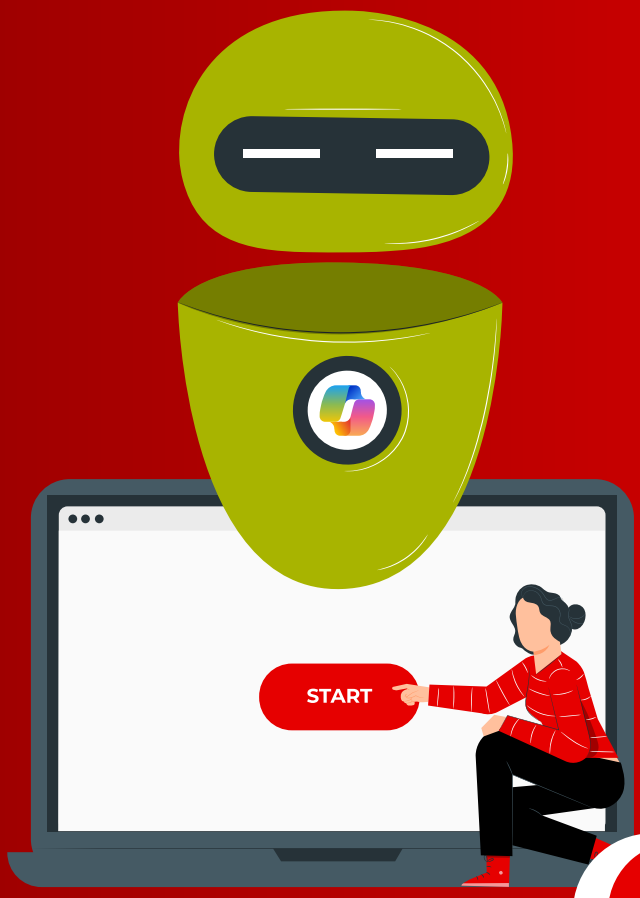
Fort Knox-level security:

Copilot follows strict compliance regulations, reducing the risk of leaks, data breaches, and legal complications.

It integrates seamlessly with your existing tools:

Copilot works within Microsoft 365 applications like Outlook, Word, and Teams, making AI a safe and powerful part of your workflow without additional risk.

Looking for a secure way to leverage AI without risking your company's data? Click here to request a call and discover how Microsoft Copilot can keep your business safe.



vodacom business


vodacom
business