

Is Your Data Copilot-Ready?

Here's the Checklist You Need

If Your Data's a Mess, Copilot Will Find It and Spill It

Microsoft Copilot helps your teams work faster, write better, and answer questions at lightning speed. But what it doesn't have is a built-in filter for data you don't want it to see.

Copilot can surface anything it has access to: Draft M&A contracts, salary history spreadsheets, confidential IP, outdated sales pitches, and even that one folder labeled "old-confidential-final-FINAL-v2."

If your sensitive data isn't classified correctly, if access isn't locked down, or if your labeling is a mess (or missing altogether), Copilot will happily pull it into a Teams chat or suggest it in a Word doc. Whoops!

So, is your data Copilot-ready? Or are you about to knight your AI assistant as the world's most efficient over-sharer?

Top Three Copilot Missteps to Avoid

1. Letting Microsoft 365 default permissions run wild, amok, or both
2. Trusting manual tags or user-driven classification
3. Assuming Copilot "knows better" about what not to expose



The Copilot-Readiness Checklist

Before you turn on Copilot across your organization, it's time to run through these must-haves:



Do you know where your sensitive data lives?

It could reside in Teams, SharePoint, OneDrive, Exchange, and anywhere else in the unstructured wild west.



Are sensitivity labels accurate and widely applied?

If they're missing, wrong, or inconsistent, Copilot has no way of knowing what's okay to surface.



Are permissions scoped to need-to-know?

Least privilege isn't a luxury. It's how you stop Copilot from feeding interns board minutes.



Can you track how Copilot is accessing and surfacing data?

Visibility is everything. You need usage monitoring, not just config dashboards.



Does your classification system understand context?

Regex won't cut it. You need AI that leverages semantics to tell a resume from a salary report.



Are you monitoring Copilot's downstream impact?

Summarized data still creates risk, especially when it's pasted into slides or shared in chat.

Your Fast Path to Copilot-Ready Confidence

1 Run semantic discovery across Microsoft 365

Find and classify sensitive data automatically and with context.

2 Automate the application of sensitivity labels at scale

No manual tagging, no inconsistencies. Label smarter, and do it much less often.

3 Monitor usage and map risk

Understand how Copilot is interacting with your data—and where it's creating exposure.

4 Create policy triggers and auto-remediation

Flag or restrict sensitive content in Copilot workflows before it becomes a headache.

Final takeaway

Copilot is only as safe as the data it's connected to. If you wouldn't want it emailed, printed, or shown in a meeting—don't let Copilot find it by accident.

**Want to test how Copilot-ready your data really is?
Request a demo today.**

Schedule a Demo

