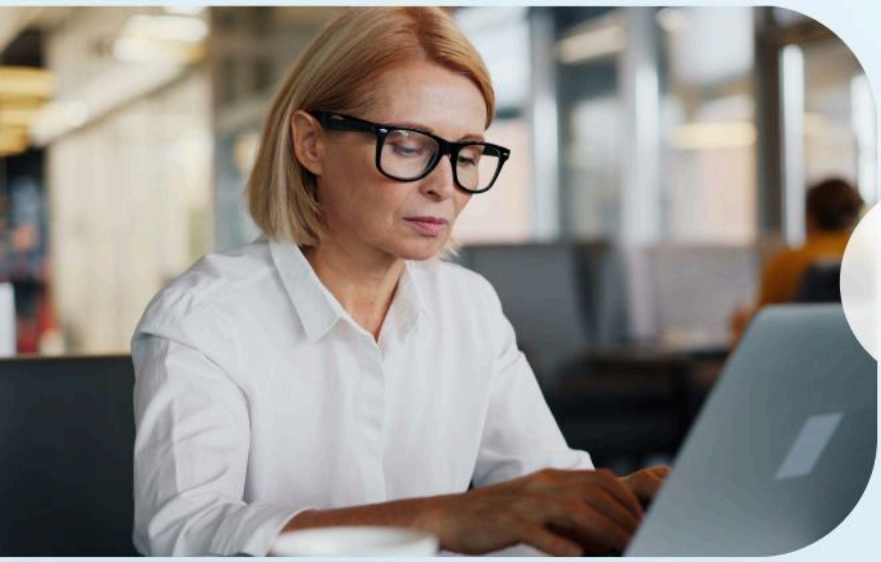
coretelligent

Follow the Data

How sensitive information moves through everyday work in financial services

Microsoft Purview + Coretelligent





Sensitive Information Is Meant to Be Used

Financial services firms hold a lot of information worth protecting. Some of it is personal or regulated. Some is confidential because of what it reveals about your firm, your clients, investors, strategies, or operations.

And people need that information to do their jobs.

Take this familiar scenario: an investor sends your firm a due diligence questionnaire (DDQ). Answering it requires information from across the business.

The answers can come from all over. Someone has to find the right information. Colleagues from different teams may need to contribute. AI may help locate source material or draft a response. Eventually, the approved information has to be shared with the investor.

→ **So, what happens to sensitive information as the team gets to work?**



The DDQ arrives. Where are the answers?

Some answers may already exist in a previous DDQ. Others might come from policies, reports, shared files or other approved sources across the firm.

Before anyone can use that information, they have to find it.

Can you identify the sensitive information your team needs to protect?

Teams need to know where sensitive information is stored and have a consistent way to recognize what requires protection. That includes personal information, along with confidential business material or information subject to specific handling requirements.

Think about how your team gathers information for the DDQ, and ask:

- **Is there a consistent way for people to recognize sensitive information?** Classification gives people and systems a common way to identify information that needs protection.
- **Do you know where that information is stored?** Sensitive material can exist across current working files, older documents, and other repositories.
- **Does the information still have the protection it requires?** Its sensitivity may stay the same even if its location or business use changes.

The answers start coming together.

Someone finds a useful response in last year's DDQ and brings it into the new one. A colleague checks the language against a current policy. Another adds updated figures from a report. A supporting document gets pulled in for reference. Comments and revisions start accumulating.

Piece by piece, information from different sources becomes part of the working response.

And as it does, its context can change. Information that started in one location may now appear in another document. More people may have access to it. Sharing settings and protections that applied to the original source may not apply in quite the same way to the working material.

How broadly is sensitive information exposed while people work with it?

The people involved may have perfectly good reasons to see the information. But access and protection need to keep up with the way that information is being used.

Think about how your DDQs develop, and ask:

- **Who has access to the working material?**
  Permissions and sharing links can leave sensitive information available to more people than the current work requires.
- **Can you identify information that's become more broadly exposed?**

Then someone turns to AI.

Instead of searching through files one by one, someone may ask Microsoft 365 Copilot to find information relevant to a question. They might use it to summarize a policy, pull key points from source material, or help draft a response based on information they already have access to.

That can save considerable time.

That speed makes it especially important to know what information people already have access to. Copilot can quickly find information a user is authorized to access, including material they may have forgotten about or wouldn't have found on their own.

What sensitive information can AI access on your behalf?

That puts more weight on the access and protection decisions your firm has already made.

Think about how your team uses Copilot and other AI tools, and ask:

- **Are the right protections in place for sensitive information used with AI?** Information doesn't stop being sensitive because someone is using AI to work with it.
- **Do you know how sensitive information is being used with AI?**

The response is ready to go.

The DDQ has been reviewed and approved. Now the investor needs it, along with any supporting materials requested during diligence.

Your firm may deliver those materials through a secure data room or another approved sharing method. Either way, sensitive information is moving beyond the people and systems that were involved in preparing it.

How do you protect sensitive information when the right people need to receive it?

Some information may require tighter controls than others. Depending on the material and how it's being shared, protections can help limit who can open it, what they can do with it, or where it can be sent.

Before materials go out, ask:

- **Do the recipients need everything being shared?**
  Review supporting materials for sensitive information that isn't necessary for the request.
- **Are the right protections applied to the information?**
  Labels, encryption, and data loss prevention policies can help keep appropriate controls in place.

Questions pop up after the DDQ is done.

Weeks or months later, someone may need to understand what happened with information used during the process. Maybe compliance needs to review an activity. Legal needs information for a request. Or the security team is investigating something unusual.

Can you tell what happened with sensitive information?

Useful records can help your team understand who interacted with information, what actions were taken, and when relevant activity occurred. If something warrants a closer look, your team may need to investigate what happened or locate and preserve information related to it.

Follow the Data

Find It → Work with It → Use It with AI → Share It → Account for It

And that's only one workflow.
Sensitive information touches many more every day.

Protecting Sensitive Information with Microsoft Purview

Microsoft Purview includes capabilities for finding, protecting, and monitoring sensitive information. Coretelligent helps you apply them to the way your firm works.

Your priority	Microsoft Purview	Coretelligent
Know what to protect	Discover and classify sensitive information. Identify potential exposure.	Assess your environment and requirements. Define protection priorities.
Protect information while people work	Apply sensitivity labels, DLP, encryption, and other controls.	Configure and test protections around your requirements and workflows.
Protect data used with AI	Identify sensitive-data exposure involving Microsoft 365 Copilot.	Configure Copilot controls, monitoring, and governance.
Know what happened	Review activity. Investigate data risks. Search and preserve relevant information.	Configure auditing and monitoring to support investigation and review.

See How Your Data Moves

Coretelligent can help you look at how sensitive information moves through your Microsoft environment and where Microsoft Purview may help protect it.

Talk to a Coretelligent expert →

About Us

Coretelligent provides scalable, industry-specific IT support, cybersecurity, governance, and AI services that lead to better, faster business outcomes. As a strategic partner, we empower you to run and grow your business without having to worry about your technology.

Contact Us | Visit coretelligent.com | Call 1-855-841-5888