opentext™

5 Things to Consider Before Making Microsoft 365 Your Only Privacy and Compliance Strategy

By Gwendoline Huret

Why Are Compliance Owners Turning to Microsoft?

Microsoft 365 is the clear market leader when it comes to data collaboration. SharePoint, Exchange, and Teams have become enterprise standards, and remote working has only solidified the trend. Employees share files and messages during video calls on Teams and use OneDrive and Office Online to create, collaborate, and share data.

Before you think of putting all your eggs—including privacy and compliance technology—in the Microsoft basket, there are some key things to consider.

Let's agree on the basics: data breaches are consistently rising in number and scandal size, and no one is left unaffected. Privacy is top of mind for anyone responsible for data management.

Data owners and compliance officers are like anyone else—they tend to go with what they know. Therefore, it should come as no surprise that more and more companies are turning to Microsoft 365 to protect and manage their information, on top of the collaboration role it already provides.

Microsoft has recognized the importance of data security and responded with privacy offerings for its solutions: users and administrators can now work with concepts such as sensitivity labels and retention schedules. In 2022, Microsoft rebranded its compliance solutions with the release of Microsoft Purview. So why are compliance and privacy add-ons to Microsoft 365 also thriving?

Whether you already have a data management solution and are looking to switch to Microsoft, or you are starting from scratch, here are five things to consider that will enhance your privacy strategy:

01 Privacy by Design

The dichotomy of data management is this: Business users want their data classified with easy access according to the projects they are working on, while data managers want their data classified according to its privacy, security, and retention requirements.

These two classification systems are contradictory. The ultimate productivity classification will allow a record to be shareable with anyone. The ultimate privacy classification will allow no one to see it. Companies must merge these two extremes to develop a workable intermediate: controlled access that is as limited as possible while still allowing optimal collaboration.

Data software can be designed either from a collaboration perspective or from a privacy perspective. A collaboration perspective will provide flexibility to users on how data is classified and accessed. In contrast, a privacy-based perspective will think first of the retention, next of the ability to share and work with the data. So which perspective is the priority?

Microsoft is a leader when it comes to information creation and collaboration. Its product design is collaboration first, not privacy first.

While Microsoft tries to turn a collaboration solution into a privacy solution, the industry's leading privacy and compliance software now must do the opposite. It has become indispensable for these compliance offerings to closely integrate with Microsoft 365 to protect the created and shared data. Some offerings specialize only in Microsoft 365, while others will protect data enterprise-wide.

These privacy add-ons to Microsoft would not exist or thrive if Microsoft were a privacy-by-design solution. The two need each other so collaboration and compliance can meet halfway.

When looking at a privacy solution, determine if the design is privacy-first. The sophistication of the solution will usually point you towards the answer. For instance, how is auto-classification handled? How advanced are the sensitive data labels? Is priority given to the end user's productivity or compliance and security?

02
Compliance Across a Hybrid Environment

I want to talk about a customer (completely anonymized in this story) who works in an industry where data privacy could be considered a matter of life or death.

Several years ago, and some Microsoft marketing later, this customer decided that Microsoft's privacy offerings would allow them to retire its existing privacy solution. They stopped investing in the historical compliance market leader they were using and went full steam towards a Microsoft 365 privacy solution—Records Center. This case study is critical because it represents the current trend we see in the market for the reasons explained in our introduction.

The first issue the customer faced was that its environment, as with most customers today, is hybrid and spread across an on-prem and Azure cloud environment. The on-prem environment is legally required in its country to manage certain types of information, so there was no plan for this environment to ever be non-hybrid. This requirement exists for many industries and geographies.

Anyone with a hybrid environment should know that Microsoft offers one privacy solution for on-prem environments and a separate one for the cloud. The two offerings must be separately implemented and do not speak to each other. In fact, it was impossible for this customer to even import or export any policies from one tool to the other.

An ideal privacy solution should have one central dashboard for policy management, which gets universally applied across all data sources. Privacy stakeholders are not usually technical. They are business users who find the source of the data almost irrelevant, a prerequisite to making strategic decisions. The information must be displayed in one place for a human brain to make sense of it.

03 The Importance of Centralized Rule Management

Not having a central dashboard to understand or report on data management is also present within each instance (cloud or on-prem) of the Microsoft 365 offering itself. We mentioned earlier that Microsoft offered various consoles for managing compliance. Whether a user is using Records Center, DLP rules, a content organizer rule, a compliance center rule, or a hold rule, these different moving parts are not reflected or reportable from one central location and are all configured and managed in different areas. An end-user, or even an admin, would struggle to understand which rules apply to what sites, let alone individual files. There is no universal reporting functionality to explain how the data is managed overall. Even with the new Purview release, the privacy design is still not regrouped, but a sum of various moving parts.

This situation takes us back to the importance of privacy by design, which is required to form a solution with one central dashboard. A collaboration-first and privacy-second solution will struggle to offer such a view. If you can't understand or report on your compliance rules, the usefulness of your compliance solution will be limited, and the solution will be highly prone to human error.

> **"If you can't understand or report on your compliance rules, the usefulness of your compliance solution will be limited, and the solution will be highly prone to human error."**

04 Enterprise-Scale Migration of Historical Data

Migrating to a Microsoft 365 compliance offering requires an enterprise-scale data migration for any content not created within it. In our real-world example above, migration became a significant issue. The customer tried migrating over 200 million records from various data sources and found that, with such high volumes, the performance delivered was not acceptable when attempting to migrate content to SharePoint. The customer specified that it had SharePoint experts on the team, and that the cost was not a concern, implying this was purely technology related.

The company attempted the migration for over a year. Performance was not satisfactory and neither was the privacy functionality. The customer concluded that migrating content from non-Microsoft sources into SharePoint was very challenging, especially with high data volumes. Metadata had to be mapped manually, and the SQL servers took a performance hit. The data sources were nothing exceptional as the data that had to be migrated was in a file system, one of the most common locations for data in a company.

Before opting for a Microsoft 365 privacy strategy, consider what impact such data migration might have on your organization and assess the quantity of data currently outside SharePoint or OneDrive. Could a manage-in-place alternative be more adaptable? Try to test or consider how such a large migration to SharePoint would work for you. Having an estimated timeframe of how long it takes your organization to import large quantities of data into SharePoint is a good start. Whatever solution you choose, managing in place and minimizing migration is usually a winning strategy.

> **“[Running and transforming is] a balancing act—but all those efforts can be meaningless if they cannot properly secure the business, its customers, and other critical assets.”**
>
> A Cyber-Resilience Model for the Next Era | Dark Reading ›

05
Human Error

The saying, "You're only as strong as your weakest link," fits compliance well. Unfortunately, when it comes to software, the weakest link is usually a human.

Customers who opt for any privacy solution should consider, "How will this change be adopted, and how will it be managed?" Hint: the best solution can run as automated as possible, with as little interaction from the end-user as manageable.

The problem of human error starts as early as the initial setup or rule configuration. When our real-life customer opted for Microsoft 365 privacy solutions, it instructed employees on how to manage records in SharePoint. In the first year, it was estimated that over half of sensitive data was not declared correctly in Records Center, due to human error. As the Records Center design in this particular use case relied on users to correctly declare content as a record before it could be managed, it left users with the responsibility of manually defining sensitive documents. A successful compliance tool will not burden the everyday end user with records management, but instead will automate processes behind the scenes.

Record managers found Records Center hard to use for setting up and running policies, leaving the customer unsure whether it was functioning correctly. They also found that with SharePoint updates, the tool sometimes stopped working. Even more frightening than records not being correctly declared, customers found that if a record admin deleted a site that contained records, Records Center did not prevent the deletion, even when confidential documents under a policy were affected.

When selecting your privacy strategy, remember that human error covers both declarations of records and rule configuration and setup. How automated is the configuration of your privacy tool? How complex is the setup? Does it work cross-site level? Does it have a central dashboard to manage policies? Setup, configuration, and daily use are all considerations for ease of use. The easier and more intuitive your solution, the lower the long-term maintenance costs, particularly when it comes to user onboarding and training.

> **"You're only as strong as your weakest link. Unfortunately, when it comes to software, the weakest link is usually a human."**

What to Look for in a Privacy Solution

The customer in our case study changed strategies and decided to return to its historical vendor. We can't all specialize in everything.

Privacy is not top of mind in Microsoft 365 design, which makes sense because they are focused on building the best collaboration tools, not compliance.

Many compliance tools on the market integrate with SharePoint. There's a reason they are thriving. Look for a tool that integrates seamlessly with automated and smart classification rules to not burden the end user. Microsoft 365 privacy companion tools should be able to manage in place, retire records from SharePoint, and manage them in a separate location. It goes without saying: look for an industry leader that offers all the compliance functionality you will need—automated but controlled deletion, flexible and smart retention schedules, and tight security. A strategic choice would be a companion that manages, not only SharePoint or Microsoft 365, but also your enterprise data in general. In the real world, data is hybrid. It's everywhere and in all kinds of formats. I recommend a unique dashboard that allows you to make sense of how you manage information and your general policies. Look for a solution that is intuitive to your admins as well as your end users.

About the Author

Gwendoline Huret has over 11 years of experience in Enterprise Software for Data Management and is now working as Product Manager at Micro Focus. She has specialized in privacy and cybersecurity since the start of the GDPR in 2016. She has worked on data management projects across the globe, from coding to sales to product management. Gwendoline has a Masters in Mathematical Engineering and is based in Madrid, Spain.

Gwendoline Huret
Product Manager, Micro Focus

Learn more on our website.
Check out our Microsoft 365 alternatives.
Request a demo.

Get in touch with your Micro Focus team.