Microsoft

Champion a human-centered approach to build a privacy resilient workplace

Foster a privacy culture and see how Microsoft Priva can help

September 2022

“By the end of 2024, three-quarters of the world’s population will have its personal data covered by modern privacy regulations.”

-State of Privacy: The Privacy Tech Driving a New Age of Data Wealth, Aug 2022, Gartner®

Table of contents

Introduction

Today, more personal data is being generated, stored, shared, analyzed, and accessed across different users, devices, and locations than ever before. In response, the landscape of data privacy regulations is continuously changing and becoming more complex. Data protection, as well as privacy regulations and laws, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have great impact around the world. They set rules for how organizations should store personal data and give people rights to manage the personal data an organization collects. Data privacy is not just about meeting compliance standards, it's also about enabling organizations to build consumer trust and protect personal data throughout the data lifecycle.

Consumers' expectations increase when there are higher levels of scrutiny toward compliance and proper data management. One issue preventing end-to-end data privacy is that employees still believe data privacy is the sole responsibility of an organization, whereas employees themselves tend to access, use, and share information across different entities. Organizations should take a "privacy by default" stance to meet regulatory requirements and develop customer trust.

At Microsoft, our mission is to empower every person and organization on the planet to achieve more. With this principle in mind, we launched Microsoft Priva, which focuses on empowering users who handle personal data to make smart data-handling decisions.

This e-book is intended for data privacy decision makers across all businesses, regardless of size, to help increase their overall awareness on data privacy. It also highlights how Microsoft Priva Privacy Risk Management can help you safeguard personal information and manage privacy risks proactively and automatically, enabling you to achieve your data privacy goals.

What makes data privacy more challenging?

What makes data privacy more challenging?

Currently, many privacy decision makers across industries are encountering challenges that make safeguarding trust in data privacy more complex and critical. Let's review some of the common challenges they're facing while assessing their data privacy posture and minimizing data privacy risks.

Challenge: Identifying personal data manually provides limited and point-in-time insights to improve privacy posture

Many organizations still use manual processes to identify personal data. They manually maintain data inventory and mapping—primarily through email, spreadsheets, and in-person communication, making the process costlier and ineffective. Also, there's often a lack of actionable insights, which would help mitigate security and privacy risks like cross-border transfers or data hoarding. Missing contextual insights could lead to undetected or unaddressed critical risks, and, in turn, potential noncompliance with privacy regulations.

Challenge: Overshared personal data usually goes undetected without routine manual audits

When employees share personal data across departments and geographies, it can result in overexposure and prolonged access to data. To comply with regulatory requirements for data access, organizations should continuously audit access to personal data and minimize access to the people who need it. Organizations are seeking a more automated approach to revoke or restrict unnecessary access to personal data, while not impeding productivity with strict policies.

Challenge: Data minimization is an ideal concept that is challenging to manually operate

Regulations like the GDPR require organizations to collect and process the minimum amount of personal data needed for a specific objective, and to delete the data after achieving that objective. With ongoing, exponential growth in data, most data owners struggle to ensure timely and systematic disposal. Additionally, privacy administrators aren't equipped with the context behind data collection and usage, preventing them from deciding when the data should be retired. To mitigate risks from unused and idle data, most organizations create company-wide policies for data disposal. However, these policies may not consider the business value of the data, which potentially results in storing personal data too long or removing personal data too soon.

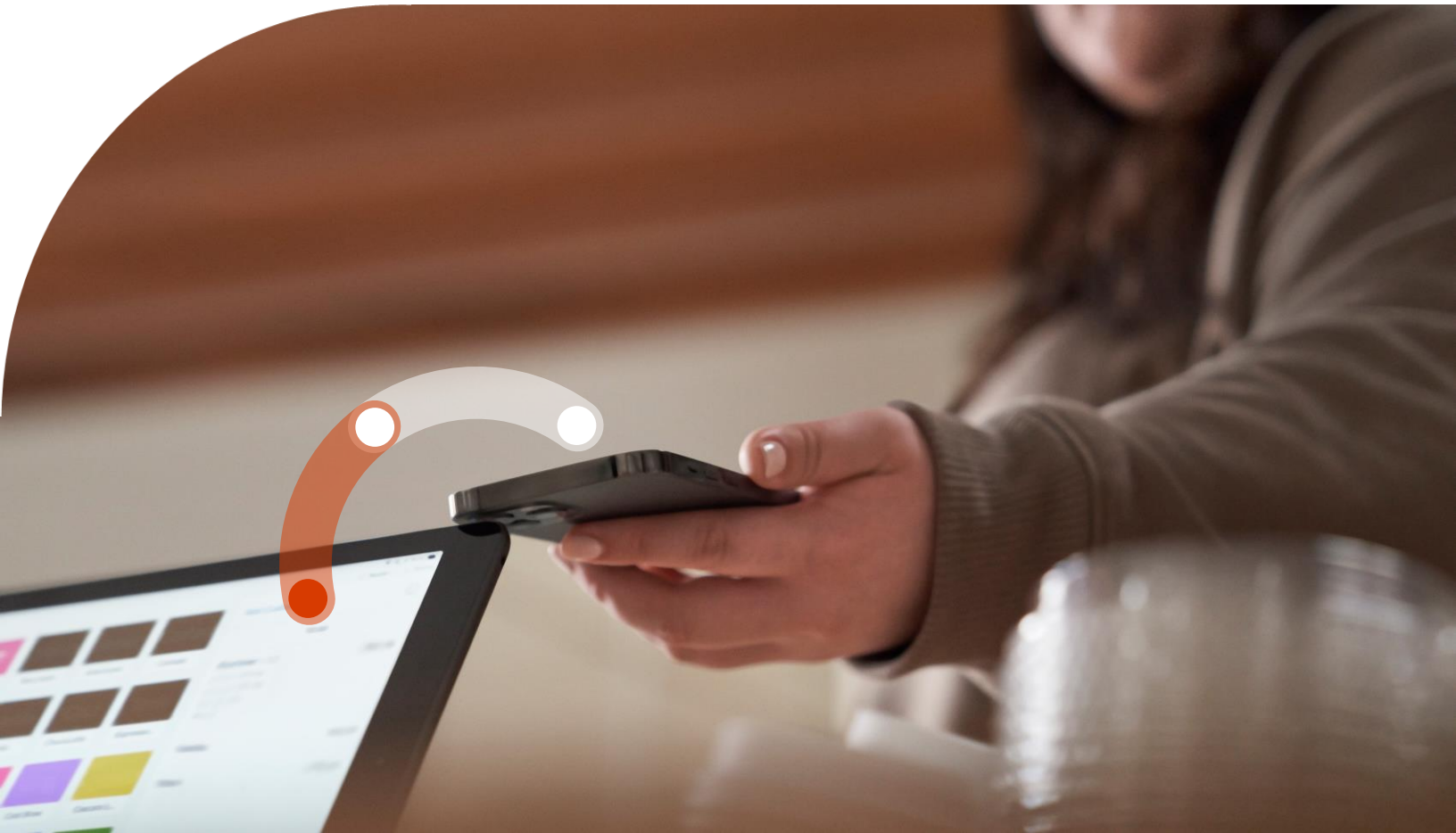
What makes data privacy more challenging? *cont.*

Challenge: Sharing data across different boundaries leaves personal data at risk

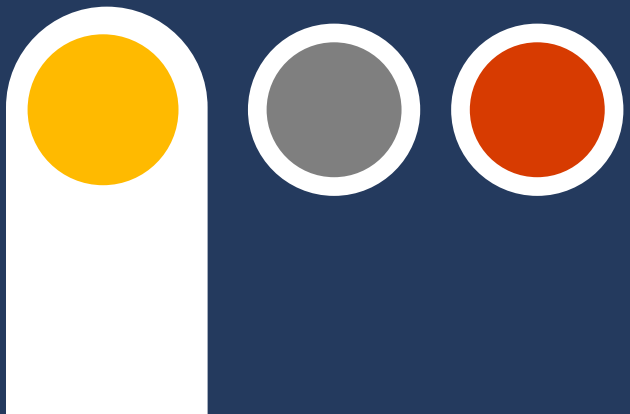
With global digitalization, most organizations are exchanging personal data across their departments and regional offices, and even with other organizations. Data privacy regulations define best practices to restrict personal data use and transfer it across different boundaries. To meet these regulatory requirements, organizations are struggling to manage data flows and maps, which rely on human judgment and assumptions regarding how data is stored and transmitted.

Challenge: Ineffective privacy readiness training leads to more privacy misconduct

Organizations don't always provide clear privacy resources for their users and employees. Annual or infrequent privacy training isn't usually effective in driving behavioral changes that last. "The Forgetting Curve," discovered by German psychologist Hermann Ebbinghaus, shows that if new information isn't applied, we'll forget about 75 percent of it after just six days. When people aren't aware of the importance of data privacy practices and their implications, they can't help protect sensitive data. These organizations are still seeking a more effective approach to training and educating users on the best practices of personal data handling.



Privacy tips and best practices



To ensure that personal data stays protected, and your organization meets the privacy regulatory requirements, you can consider some of the below data privacy tips. These can not only help you strengthen your organizational privacy posture, but also help your organization empower employees to understand the importance of data privacy and take proactive measures that reduce data privacy risks.

Replace surveys with automated data classification

Instead of sending surveys to learn where your personal data is located, consider working with your CISO or IT staff to apply auto-classification to create your data map or inventory. Use these insights as the foundation of your privacy program.

Democratize privacy best practices

Employees who process or handle personal data are your biggest allies in building a successful privacy program. Invest in a privacy readiness program and measure its effectiveness so you don't just check the box for completing an annual privacy training.

Move from a cost-driven approach to a value-driven one

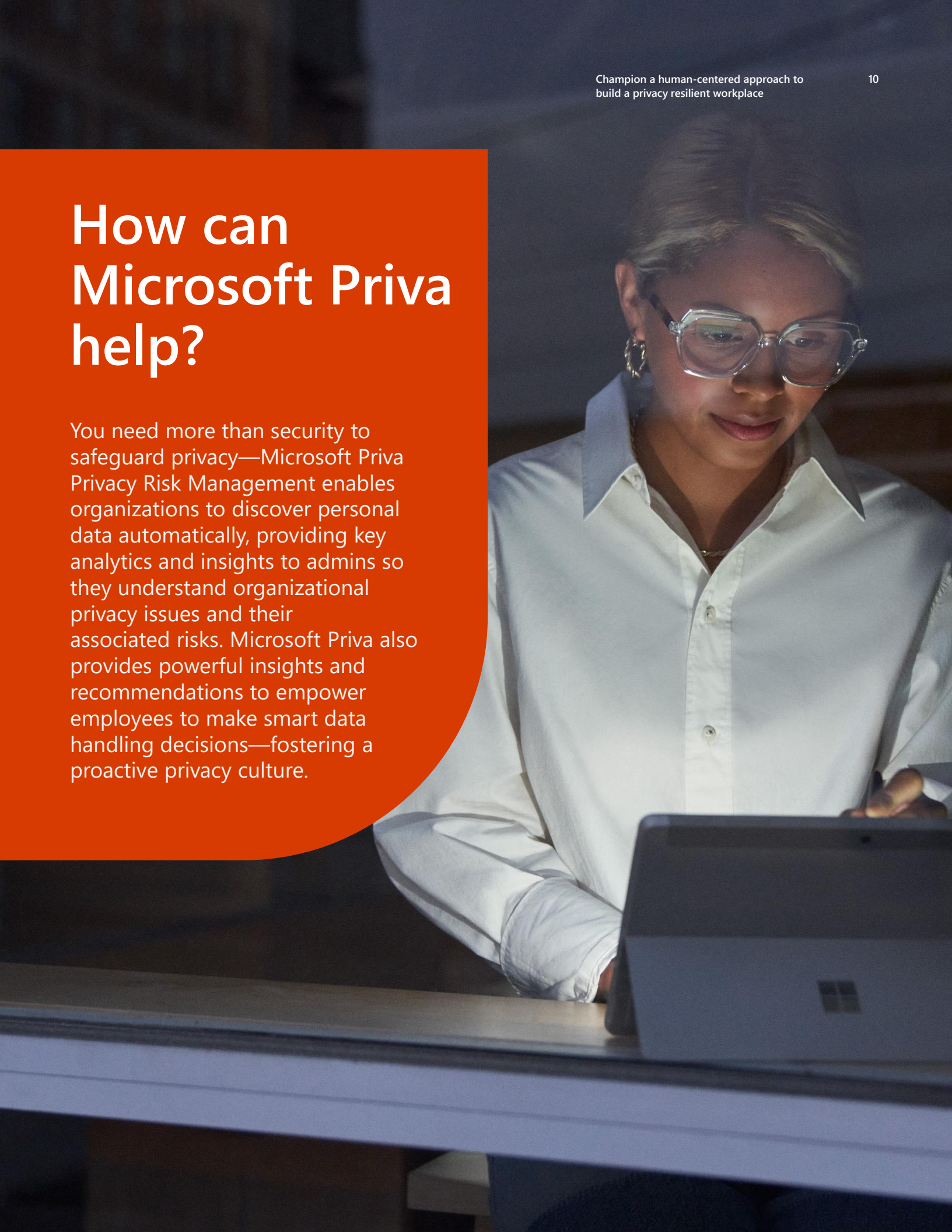
Avoid viewing data privacy as a compliance checklist. Instead, consider privacy a fundamental right while viewing compliance practices as necessary steps along the way. This helps you add value to your business instead of cost while you position your privacy program.

Address privacy risks continuously

Proactively find risks to reduce potential privacy incidents, rather than relying on periodical audits. Continuously mitigate the identifying risks to enhance your privacy programs accordingly.

How can Microsoft Priva help?

You need more than security to safeguard privacy—Microsoft Priva Privacy Risk Management enables organizations to discover personal data automatically, providing key analytics and insights to admins so they understand organizational privacy issues and their associated risks. Microsoft Priva also provides powerful insights and recommendations to empower employees to make smart data handling decisions—fostering a proactive privacy culture.



Identify personal data and risks

Instead of relying on surveys and manually updated spreadsheets, with Microsoft Priva, organizations can discover personal data through automation. But discovering personal data isn't enough—organizations need visibility into associated risks around the data. Priva Privacy Risk Management allows you to create policies from built-in templates with default configurations. Alternatively, you can create custom policies to define your conditions, alerts, and notifications. These policies are intended as internal guides and can help you:

Detect overexposed personal data so that users can secure it.

Spot and limit personal data transfers across departments or regional borders.

Identify and reduce the amount of unused personal data you store.

Key Benefit:

Gain visibility into personal data and associated data privacy risks due to overexposure, hoarding, and transfers with the help of automated data discovery and correlated risk signals.

As shown in Figure 1, Microsoft Priva Privacy Risk Management also helps identify critical privacy risks arising from data overexposure, data hoarding, or cross-border data transfers.

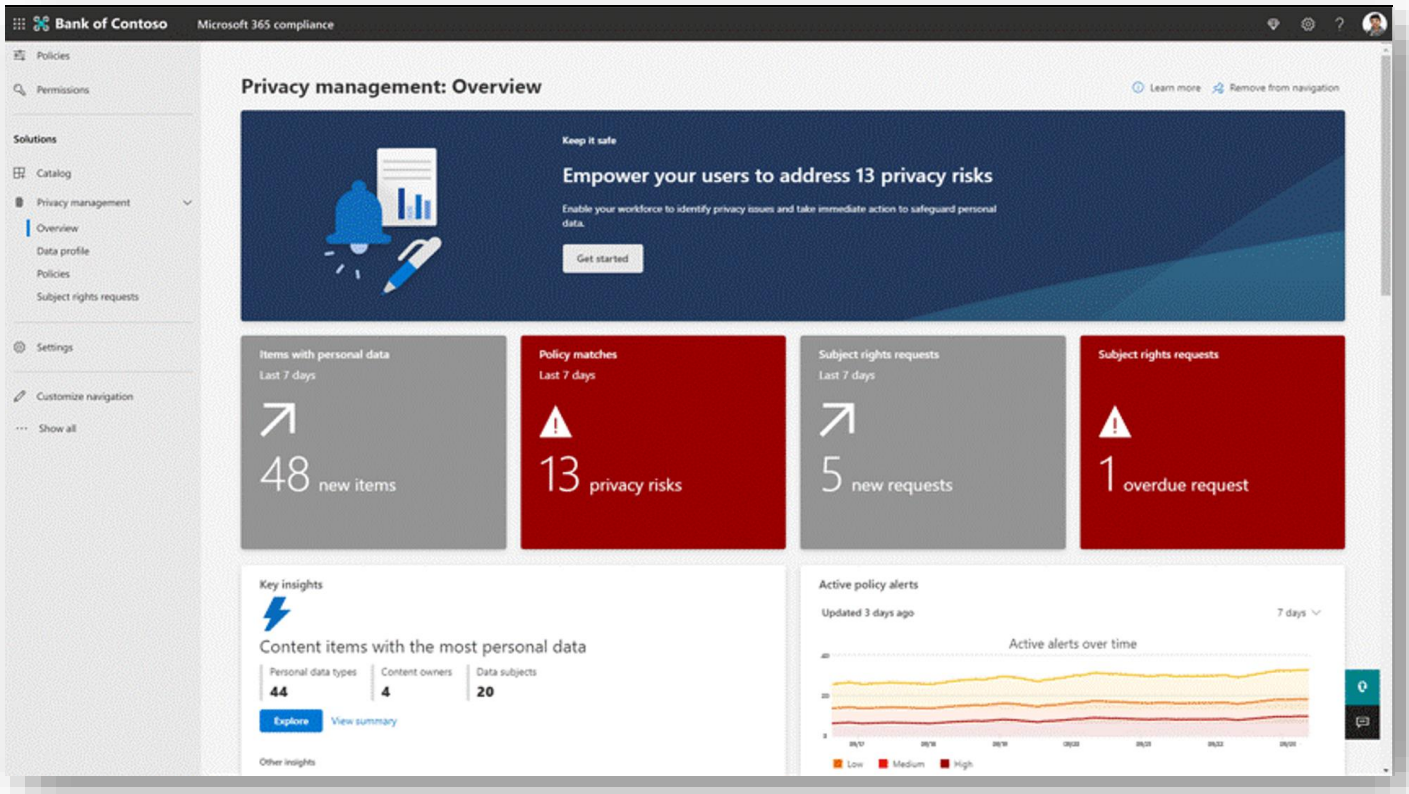


Figure 1:
Overview dashboard showcasing privacy risks and trends

Automate mitigation and prevent privacy incidents

Once these risks are identified, organizations still struggle to determine what actions they can take to mitigate the risks. To address these risks, companies may use many developer resources to build APIs that plug into different information security and governance solutions, but this method isn't efficient since context about the data can get lost in translation. **With Microsoft Priva, organizations can automate their privacy mitigation and leverage the built-in controls.** The solution provides customizable and out-of-box policy templates for data overexposure, data minimization, and data transfers.

Key benefit:

With automated policies and recommended user actions, admins can mitigate privacy risks effectively and prevent privacy incidents.

As Figure 2 demonstrates, in Microsoft Teams, a commonly used communication platform, users can receive nearly real-time notifications and guidance when sending personal data across regions or departments

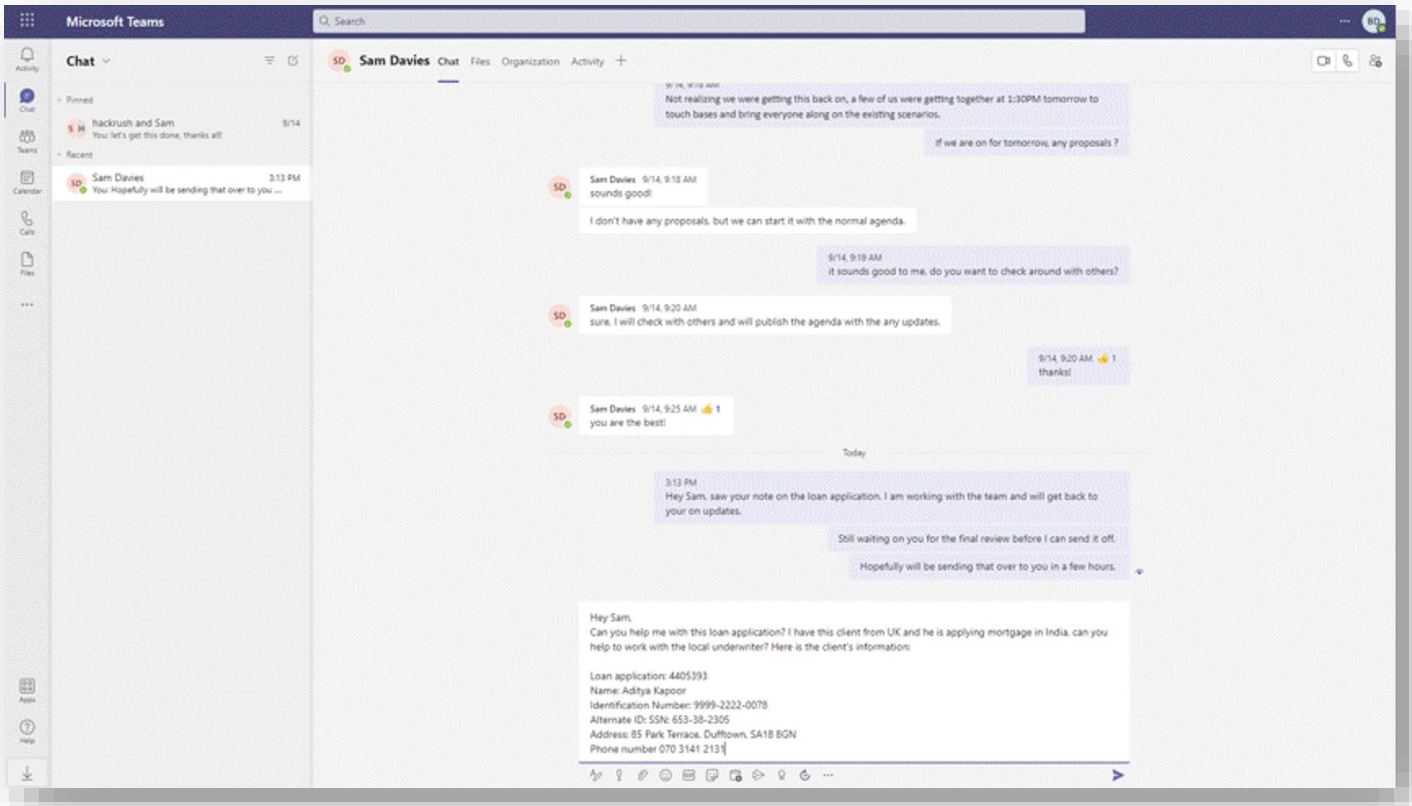


Figure 2:
A notification from Microsoft Teams about a blocked message due to organization policy

Empower employees to make smart data-handling decisions

To build a privacy-resilient culture, you need to increase awareness and accountability toward privacy risks without hindering employee productivity. Microsoft Priva empowers employees to make smart data-handling decisions by equipping organizations with a set of tools to detect data risks and establishes processes for remediation—directly notifying users about issues and recommended action items.

Employees can mitigate data overexposure or data minimization policy risks right within their everyday tools without skipping a beat. These powerful insights provide recommendations and can even direct employees to company training materials right in their flow of work, making lasting impact that helps build a privacy resilient workplace.

Key benefit

Foster a proactive privacy culture by increasing awareness and accountability for addressing privacy risks without hindering employee productivity.

As shown in Figure 3, data owners are given recommended actions, training, and tips to make smart data-handling decisions, eliminating the need to choose between privacy and productivity.

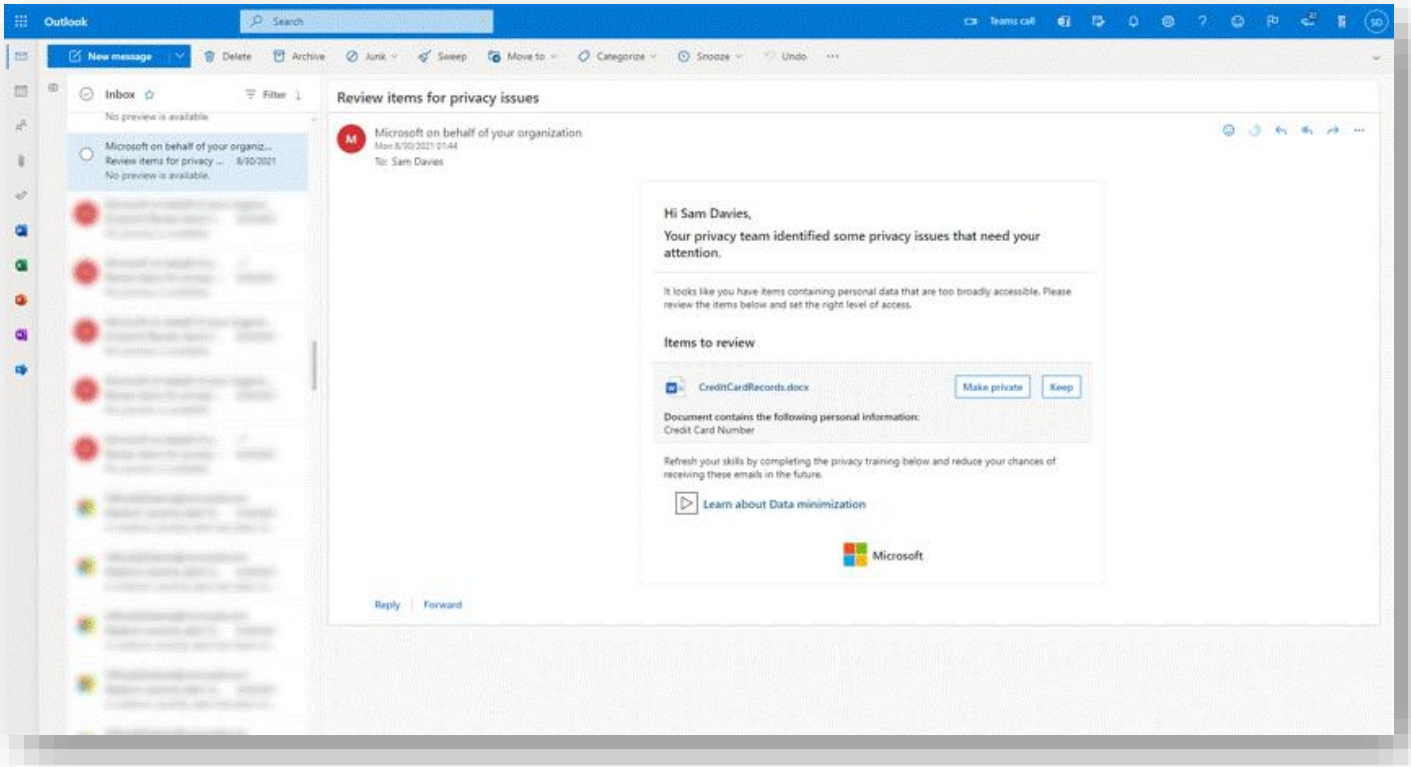


Figure 3:
Email notification showing recommendations to mitigate the potential risk associated with personal data

Build a privacy resilient workplace with Microsoft Priva

Microsoft is excited to help you on your privacy journey—we hope the knowledge in this e-book leads you toward taking a proactive approach in your privacy posture. To get started with Microsoft Priva, you can learn more about the solution in our technical documentation and try Priva Privacy Risk Management for 90 days at no cost.

Start your free trial today

Go to aka.ms/privatrial to start your free trial