Priva Risk Management

What is it	Where is it and what to do
To meet regulatory requirements, we must instill good practice across the organization,identify non-compliant behaviors, and correct them to plug any gaps. Privacy violations are not limited to data breaches from external hackers or intentional malicious acts.They can also be the result of human error and mishandling of data. Priva Risk Management is designed to help you uncover non-compliant behavior and improve the company culture and behavior around personal data.	Navigate to https://compliance.microsoft.com From the left side navigation menu, click on **Priva Privacy Risk Management** to expand the menu, then click on **Overview**
With Microsoft Priva, you can gain insights into private data stored in your Microsoft 365 environments. This solution will evaluate your data for personal information, give you a clear view of what you store, and offer opportunities to investigate areas of key interest. First, we will begin by accessing the Priva Overview screen in the Microsoft 365 Compliance Center. The Priva Overview screen is a dashboard that provides dynamic insights about the personal data stored in your Microsoft 365 environment to help you quickly spot issues, identify risk indicators, and take action to fix issues. A few key features we would like to highlight are: **Items with personal data**: Provides a count of items found, and links into a view where you can explore further details about this content. **Policy matches**: Stats on potential matches to your policies. This links you to your Policies page for further information and to take steps to handle the identified issues. **Subject rights requests**: Highlights new requests to be completed and any overdue requests. Links to the Subject rights requests page for further info. **Key insights**: These sections guide you to investigate areas of interest, like which specific content types contain the most personal data, or	1. On the **Overview** page hover over each box: • **Items with personal data** • **Policy matches** • **Subject rights requests** • **Key insights** • **Active policy alerts**

What is it	Where is it and what to do
which users are associated with the most policy matches. **Active policy alerts**: Graphs results of the alerts that you have set in the Policies section that may require attention.	
Let's first explore the personal data overview page. We can see every file that has been identified for containing privacy concerns. From here we can see the files and open a sample of the file to see the privacy concerns. We can also click on the Details section to see the exact data that is contained within a file. The data profile page gives you a high-level view of your organization's data. Here we can see the most common areas where private information is sent, as well as type of private information. Exploring these areas will provide a deeper dive into your folders and files for further investigation. Here is an example of the kinds of data Priva can find. You can see the document itself, the location, owner, and personal data types found. On the left we can see all the various types of Private information that have been flagged by Priva. If we wanted to see a breakdown of all the sensitive information displayed within the contents of one of these files, we can click here to see the information at a quick glance, without needing to open the file.	Next, navigate to the **Data Profile** page. 1. Hover your cursor over **Personal data type instances detected in Microsoft 365 locations** 2. Hover your cursor over **Top personal data types across your organization** 3. Click **Explore** on the **Personal data type instances detected in Microsoft 365 locations** card 4. Double click on the **SharePoint** folder 5. Double click on one of the Files 6. Hover over the **Sensitive info type list** next to the file name
The Policies screen shows policy status with alerts & issues along with a searchable & filterable list of policies. The policy templates cover common data handling scenarios that pose risks. They empower employees to address privacy issues in the moment and to develop better data handling skills for the future. When a policy match is detected, data owners can be guided to fix problems directly with an email notification. You can also include a link to recommended privacy training. Customizable features allow you to set conditions for matches, alerts, and employee notifications.	1. On the left navigation pane, under **Priva** click on **Policies** 2. In the **Alerts** box, move along the horizontal axis to show the number of alerts over time 3. Click on **View alerts** to show the recent alerts 4. Click on the first alert in the list to show details 5. Click on the **Content tab** to see the actual item that triggered the alert

What is it	Where is it and what to do
Here in the alerts section, we can see a timeline of the last 30 days of Alerts. Let’s look at what some of these alerts entail by clicking on the View alerts button. Here in the Alerts detail page, we can see a breakdown of the different alert statuses, the same timeline from earlier, as well as a list of alerts. Let’s open one of the alerts in the list to see what triggered it. From here, we can see a general overview of the alert that includes the policy that was matched and when the alert was created. If we want to see which file caused the policy match, we can open the content tab. This will show us a list of the files that were matched with our policy. From this screen, the privacy admin can evaluate the alerts and decide if they want to turn them into issues for further investigation. Because we can see the actual files, the admin can see what caused the alert to judge the severity of the violation. After an issue is created from an alert, the status can be tracked, severity can be assigned, and other people can be added to follow the issue. If we wanted to assign a severity level to our issue, we could do that as well. And finally, once we have tracked the issue, determined the severity, and appropriately followed up, we can resolve our issue. Once we click resolve, we can write out the steps we took to resolve the issue for future reference.	6. Hover over the **Personal data types** to show the types in violation 7. Click **Create issue** 8. Click **Cancel** 9. Click **Close** 10. Click the browser **back arrow** to return to the **Policies** page 11. In the **Issues box**, hover over the circle to see the count of Active and Dismissed Issues 12. Click **View issues** to see recent issues. 13. Click on one of the **issues** 14. Click **Review content** 15. Hover your cursor over one of the files 16. Click the **Overview** tab 17. Click **Assign severity** 18. Click the **Choose severity** dropdown 19. Hover over **High, Medium, Low** 20. Click **Cancel** 21. Click **Resolve** 22. Click **Close** On the left navigation bar click **Policies**
The first time you access Priva three policies will be automatically initiated, one for Data overexposure, one for Data transfers, and one for Data minimization. Additionally, customized policies may be created using a collection of templates.	23. Confirm that **Data transfers** is the only option selected 24. In the **Name** box type “Data Transfer Policy<today’s Date>” 25. Click **Next**

What is it	Where is it and what to do
For this example, we will start a new policy using the Data transfers template and add a few modifications. Let's add a new, unique name to this policy but leave the description as is. On the Choose data to monitor step, we can see all the various types of personal data we will be able to monitor. We can utilize existing classification groups to automatically select different types of data, or we can individually select the types of data we want to monitor. We will start this policy in test mode so you can preview how it works. It looks for matches from the last 30 days using default settings. As data comes in, you will see insights such as how many users are affected, the types of personal data transferred, and from which locations. In this step, we can select which users or groups will be covered under this Policy. We can either select All Users and Groups, or we can pick and choose specific users and groups. For now, we will leave this setting as is to cover all users and groups. Here we can determine the scope of our policy and set which methods of sharing we wish to monitor. Now we can set which interdepartmental or international data transfers need to be monitored. For now, we will set our policy to monitor for sensitive data shared between the finance and operations teams. By checking the policy tip and recommendations box, we will be able to educate and inform our employees whenever they try to send personal data. We will also to add a link to the automated email that will be sent. By doing this, we can send our employees links to training and data protection courses to prevent further issues.	26. Select **Classification Groups**, 27. Click **+ Add classification groups** 28. Hover over the options in this list 29. Click **Cancel** 30. Click **Next** 31. Choose **All users and groups** **32.** Click **Next** 33. On the **Choose data locations to apply the policy** step ensure that: **Exchange email, OneDrive accounts, Teams chat and channel messages, and SharePoint sites** are all selected 34. Make sure **All SharePoint sites** is selected 35. Click **Next** **36.** Select **Transfers between departments in your organization** Click **+Select sender department** 37. Select **Engineering** 38. click **Add** 39. Click **+Select recipient departments** 40. Select **Sales** **41.** Click **Add** 42. Click **Next** 43. Ensure that **When content matches the policy condition, give users policy tips and recommendations** and **Send a notification email to the user**

What is it	Where is it and what to do
On this step of the policy creation tool, we can choose how often Privacy admins will be notified of the Policy matches within their company. For this policy, we will set this to 'Do not alert' We will leave testing mode turned on for this policy so that we can test this policy without alerting anybody and make sure that it is working the way we intended. On this last page of the Policy creation wizard, we can double check and edit the policy to ensure we have the correct configuration. Normally you would click Submit', but since this policy already exists, I am going to click 'Cance'l.	**when a policy match occurs** are both checked 44. Under **Choose frequency of notifications**, check **Daily** 45. Add https://aka.ms/learn as the **Link to privacy training** 46. Click **Next** 47. Make sure **Create alerts** is set to **Off** 48. Click **Next** **49.** Toggle **Run in test** mode to **On** **50.** Click **Next** 51. Review the policy settings you have just entered and click **Cancel** 52. Click **Yes**