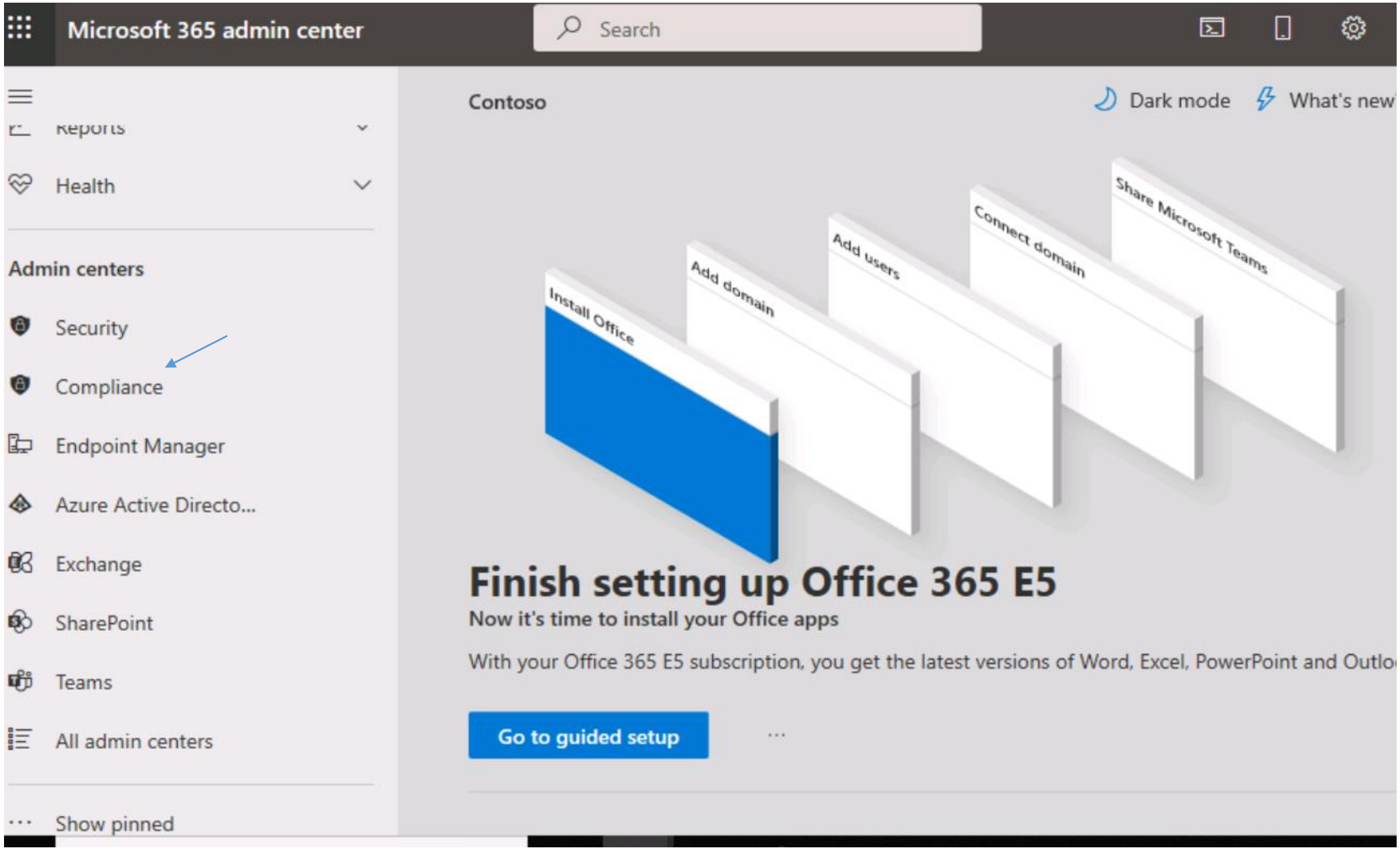
Configuring new sensitivity labels, publishing labels, creating policy


Microsoft 365 admin center
Search
Contoso
Dark mode
What's new
Reports
Health
Admin centers
Security
Compliance
Endpoint Manager
Azure Active Directo...
Exchange
SharePoint
Teams
All admin centers
Show pinned
Install Office
Add domain
Add users
Connect domain
Share Microsoft Teams
Finish setting up Office 365 E5
Now it's time to install your Office apps
With your Office 365 E5 subscription, you get the latest versions of Word, Excel, PowerPoint and Outlo
Go to guided setup

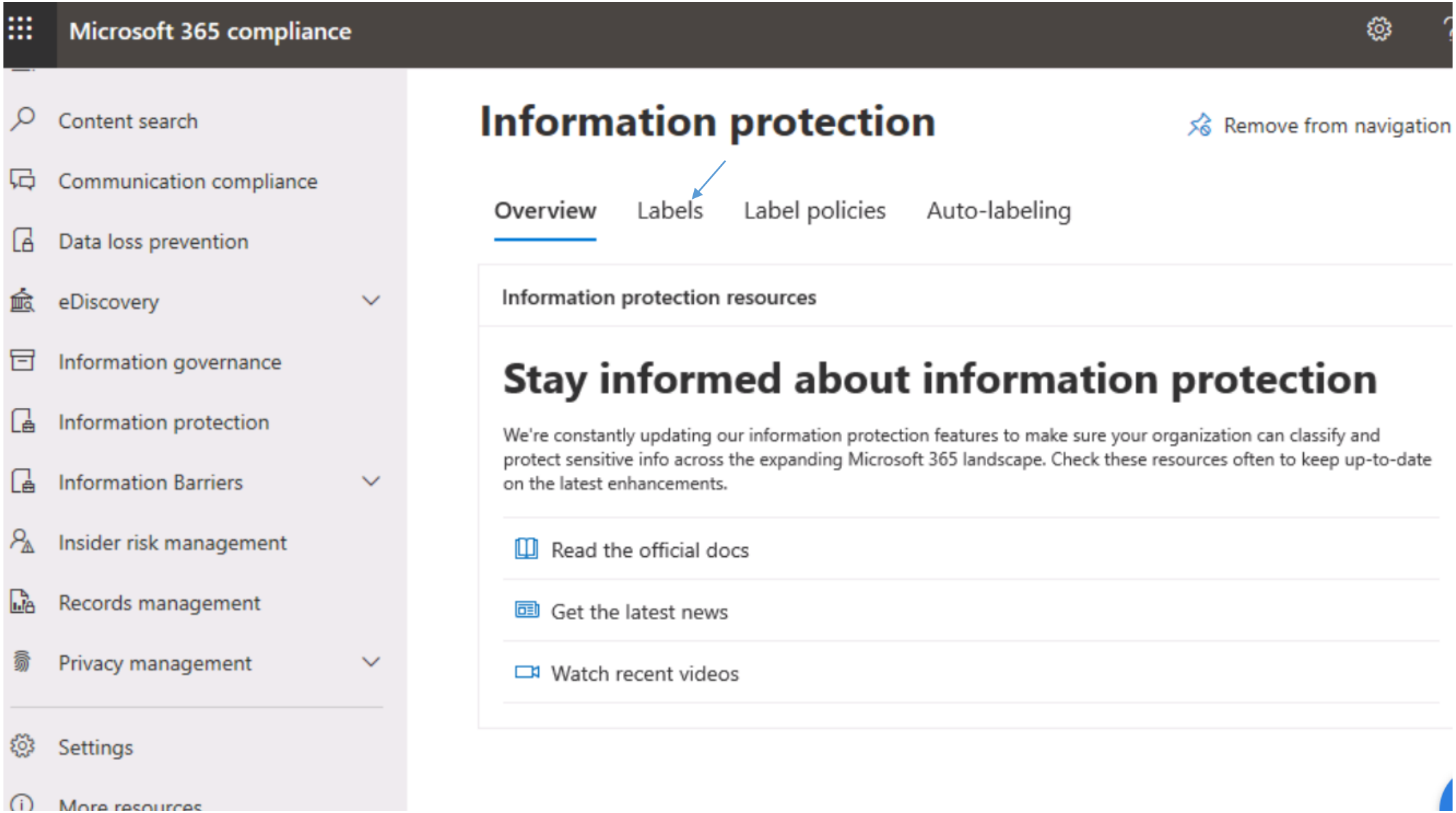
Microsoft 365 compliance

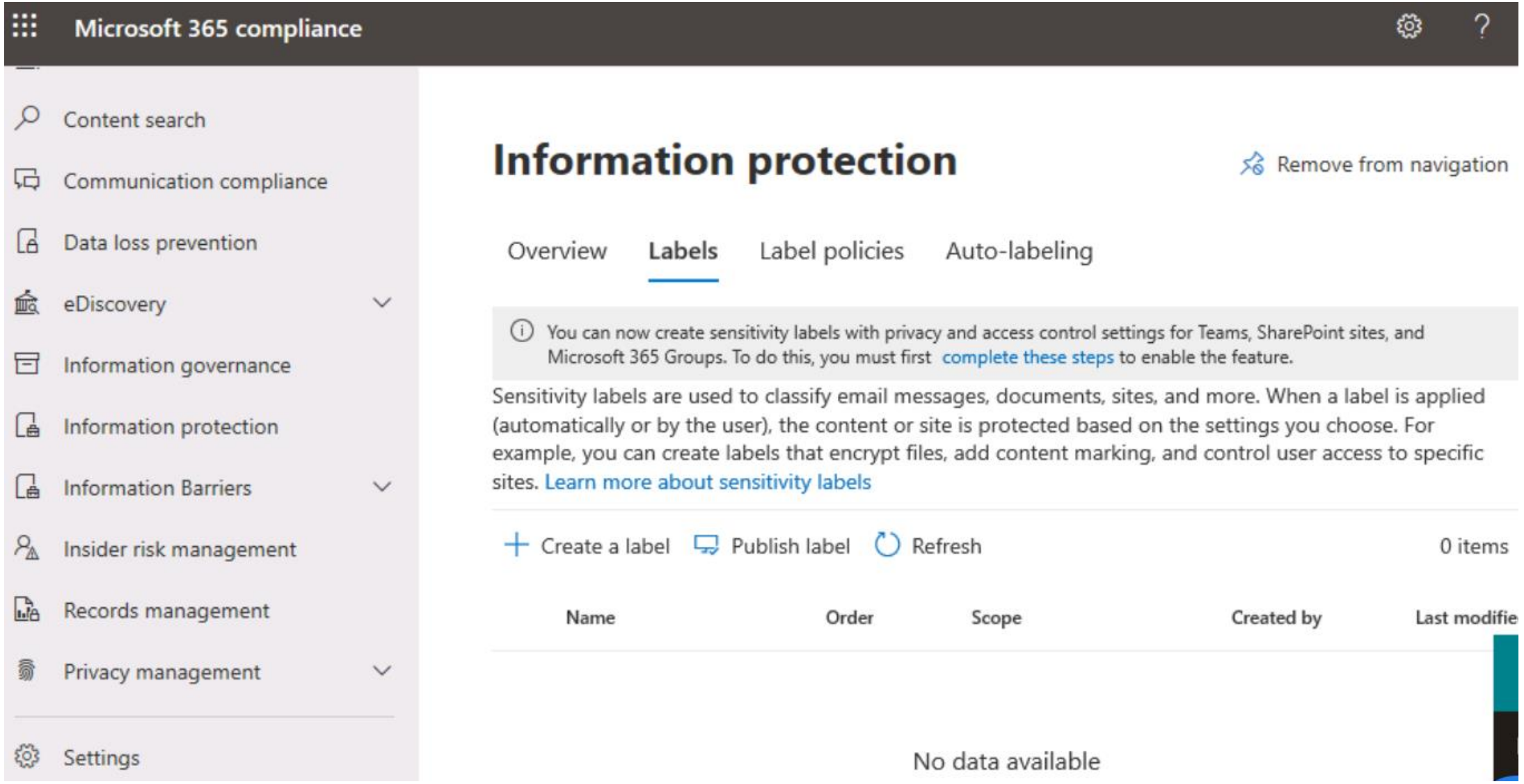
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Information governance
- Information protection
- Information Barriers
- Insider risk management
- Records management
- Privacy management
- Settings
- More resources

Home

Welcome to the Microsoft 365 compliance center

Intro Next steps Give feedback


Microsoft 365 compliance
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Information Barriers
Insider risk management
Records management
Privacy management
Settings
More resources
Information protection
Remove from navigation
Overview
Labels
Label policies
Auto-labeling
Information protection resources
Stay informed about information protection
We're constantly updating our information protection features to make sure your organization can classify and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.
Read the official docs
Get the latest news
Watch recent videos


Microsoft 365 compliance
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Information Barriers
Insider risk management
Records management
Privacy management
Settings
Information protection
Remove from navigation
Overview
Labels
Label policies
Auto-labeling
You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.
Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels
Create a label
Publish label
Refresh
0 items
Name
Order
Scope
Created by
Last modifie
No data available

New sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Schematized data assets (pr...
- Finish

Name and create a tooltip for your label

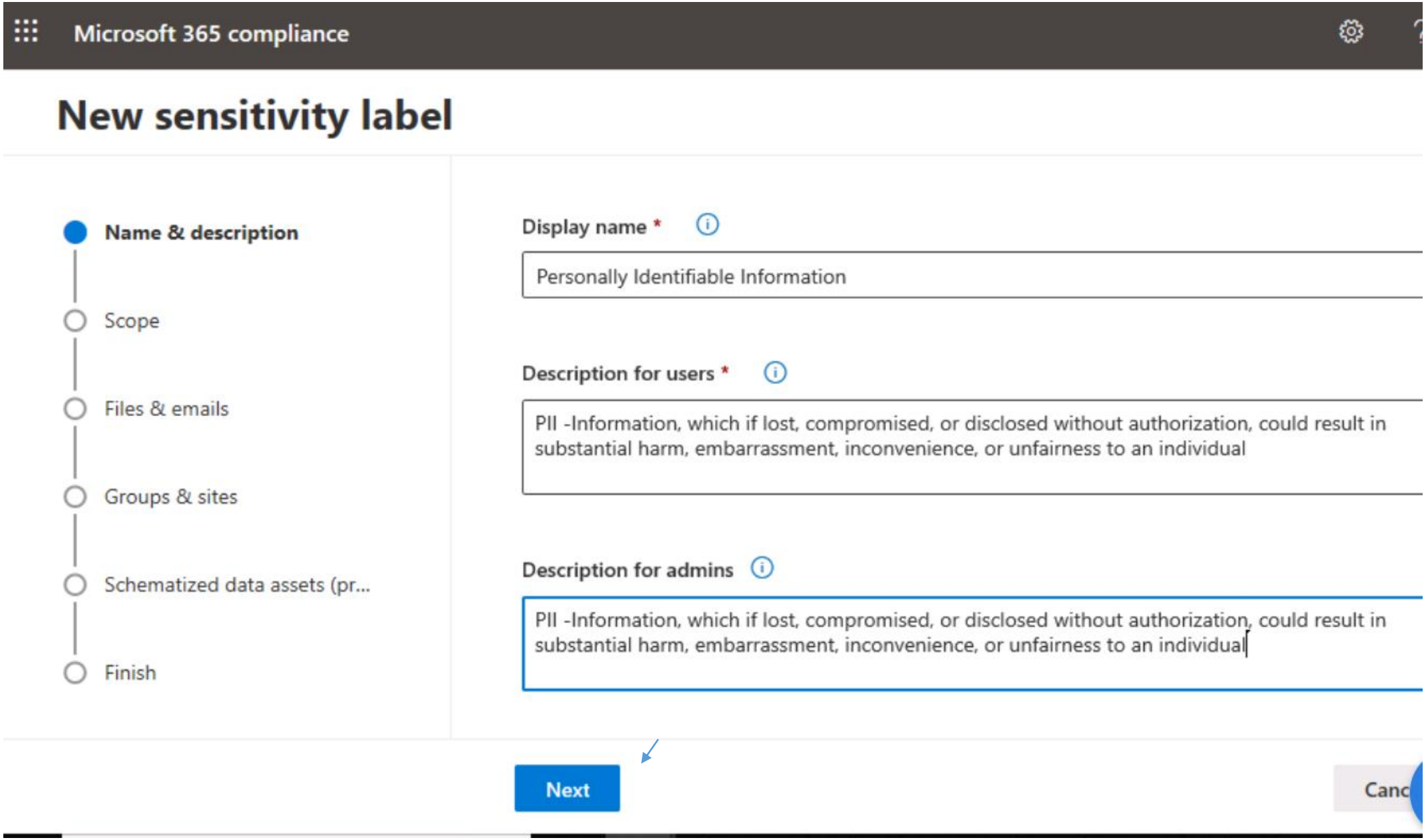
The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

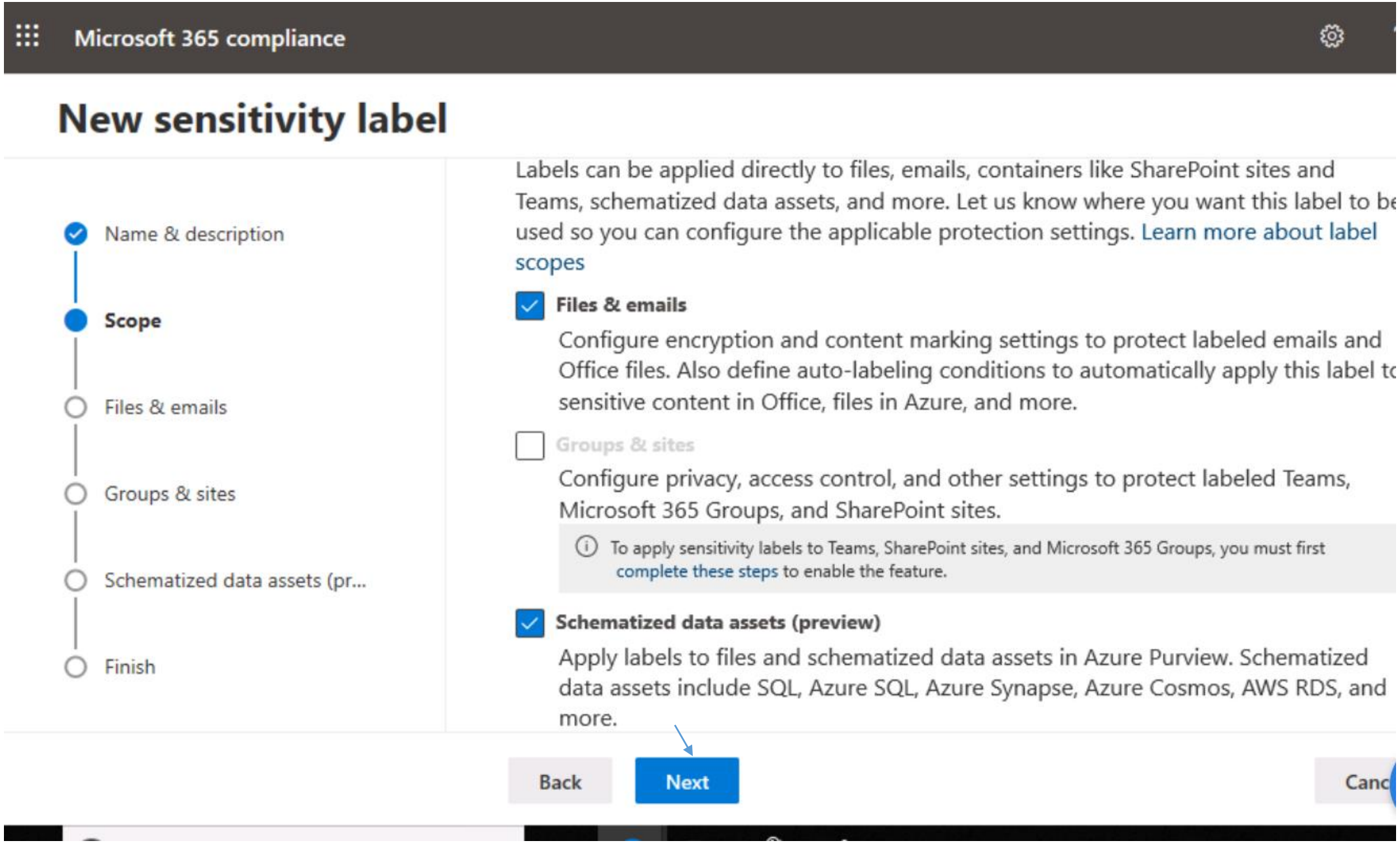
Name *

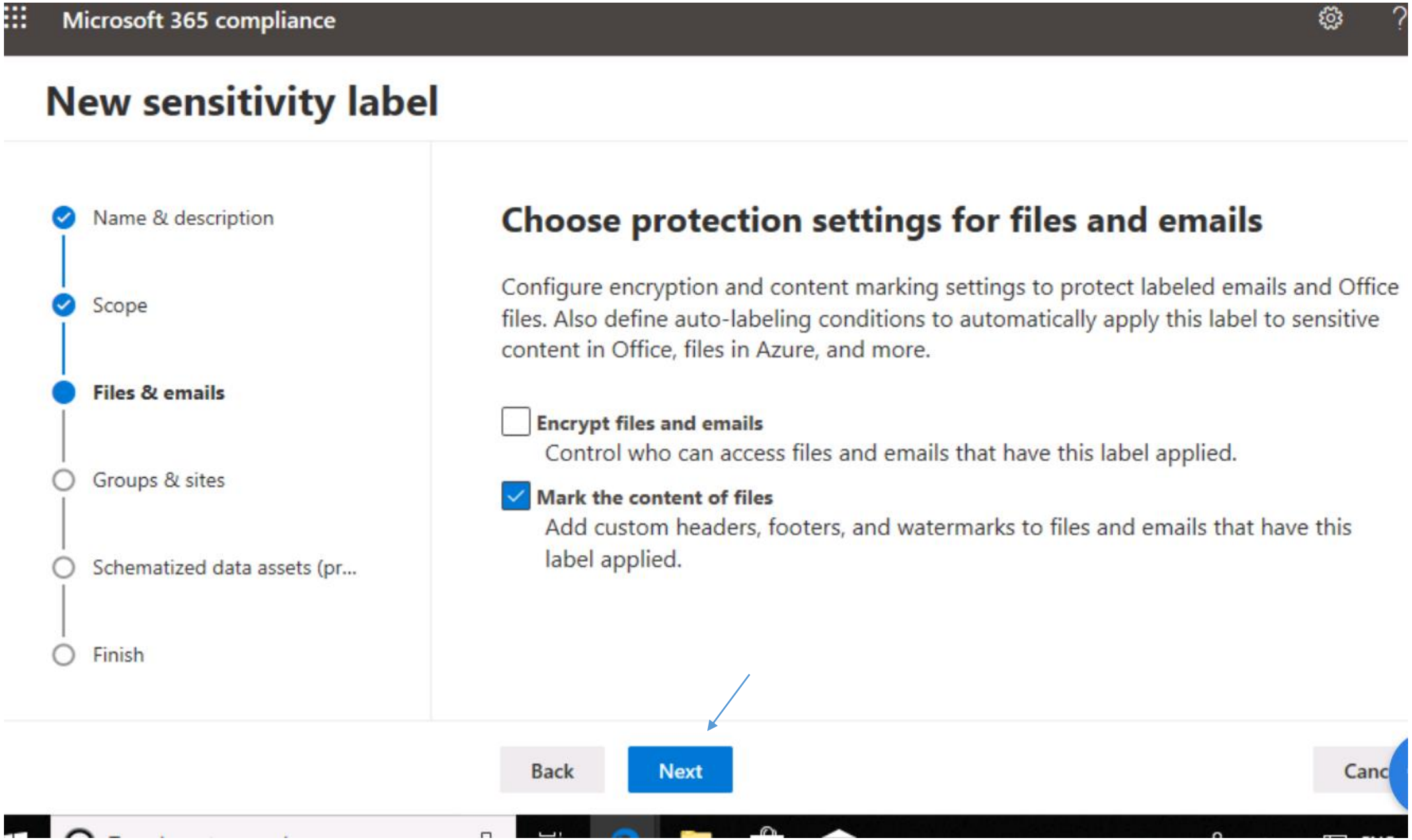
PII label

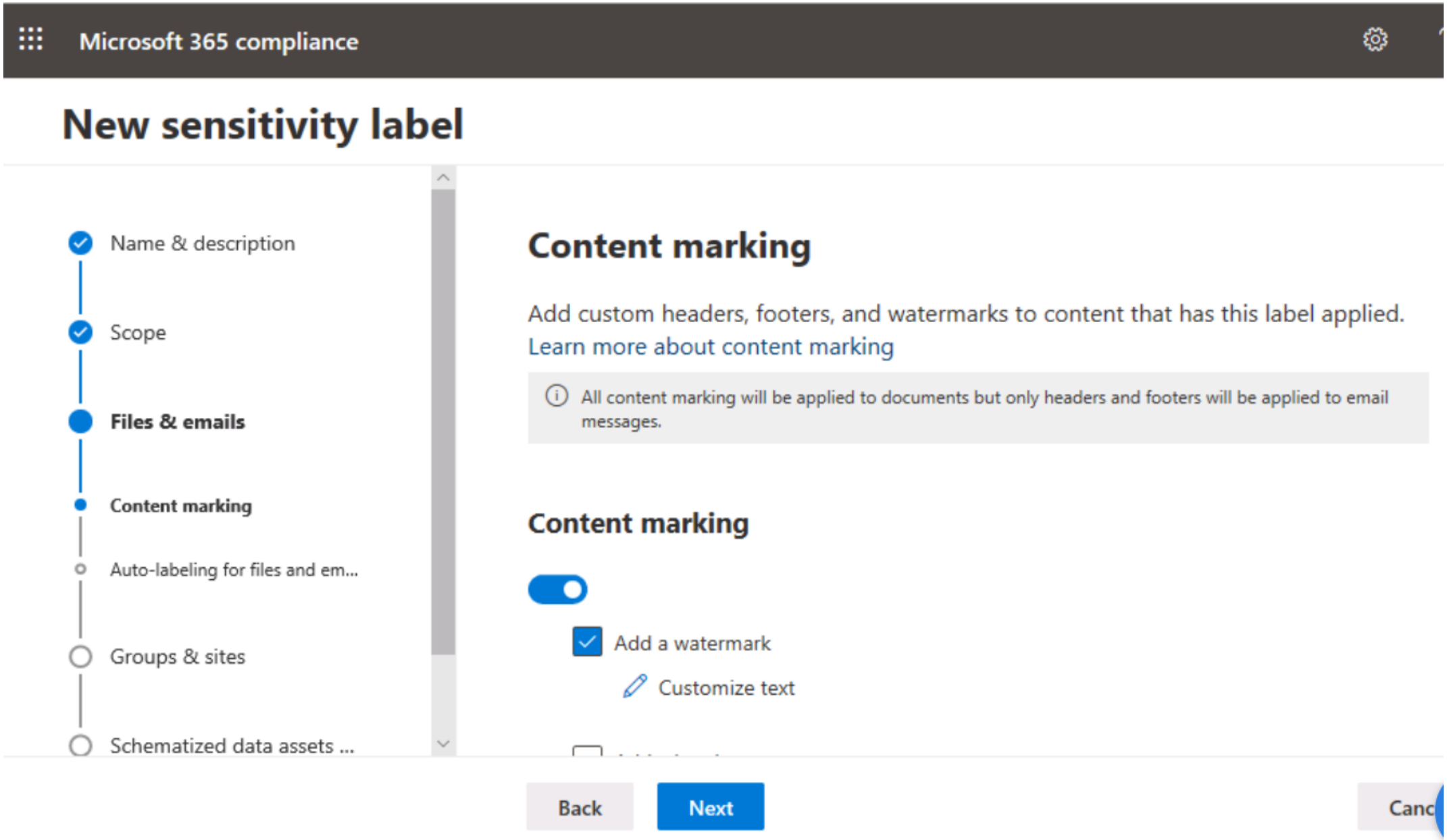
Display name *

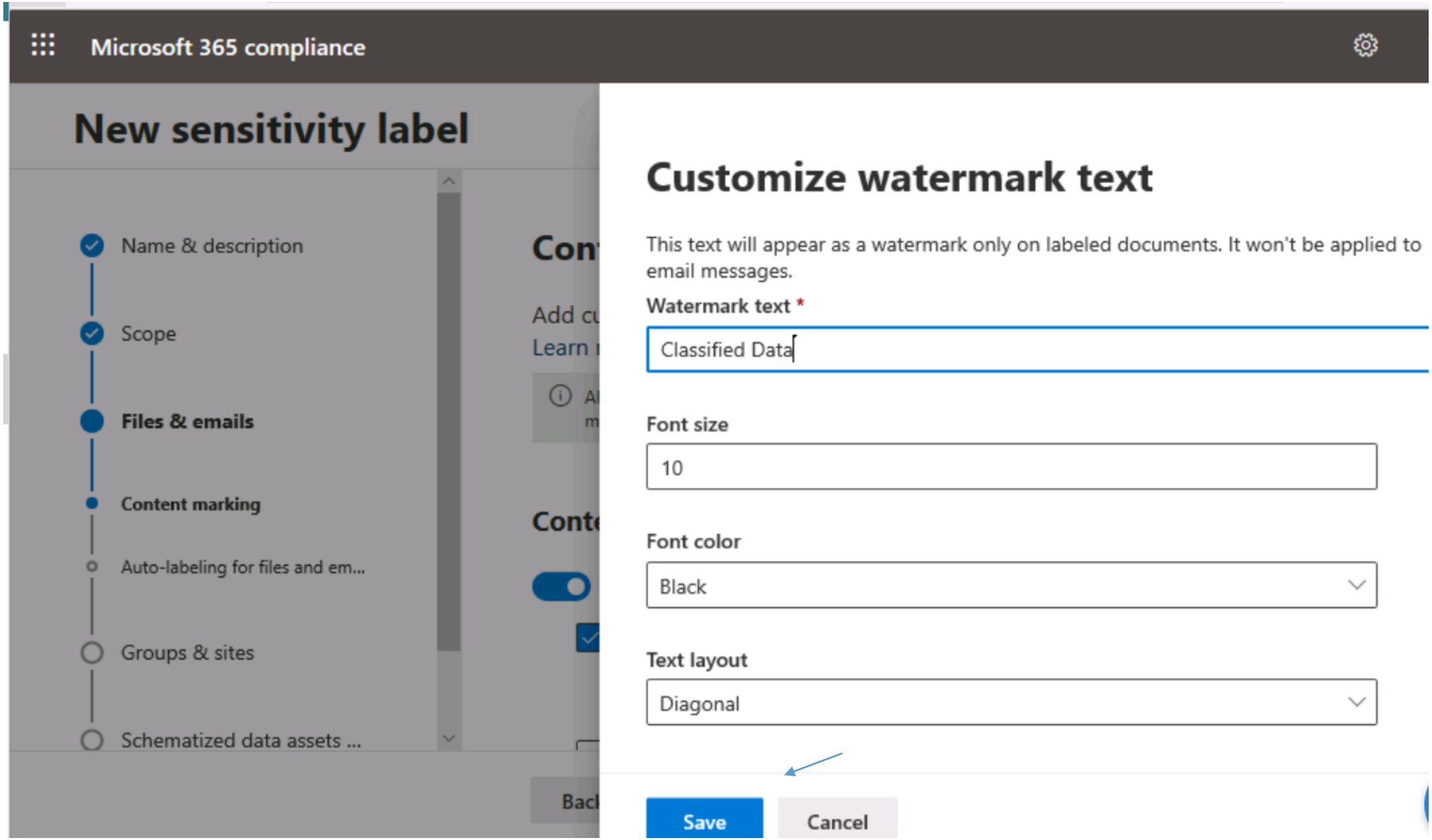
Personally Identifiable Information

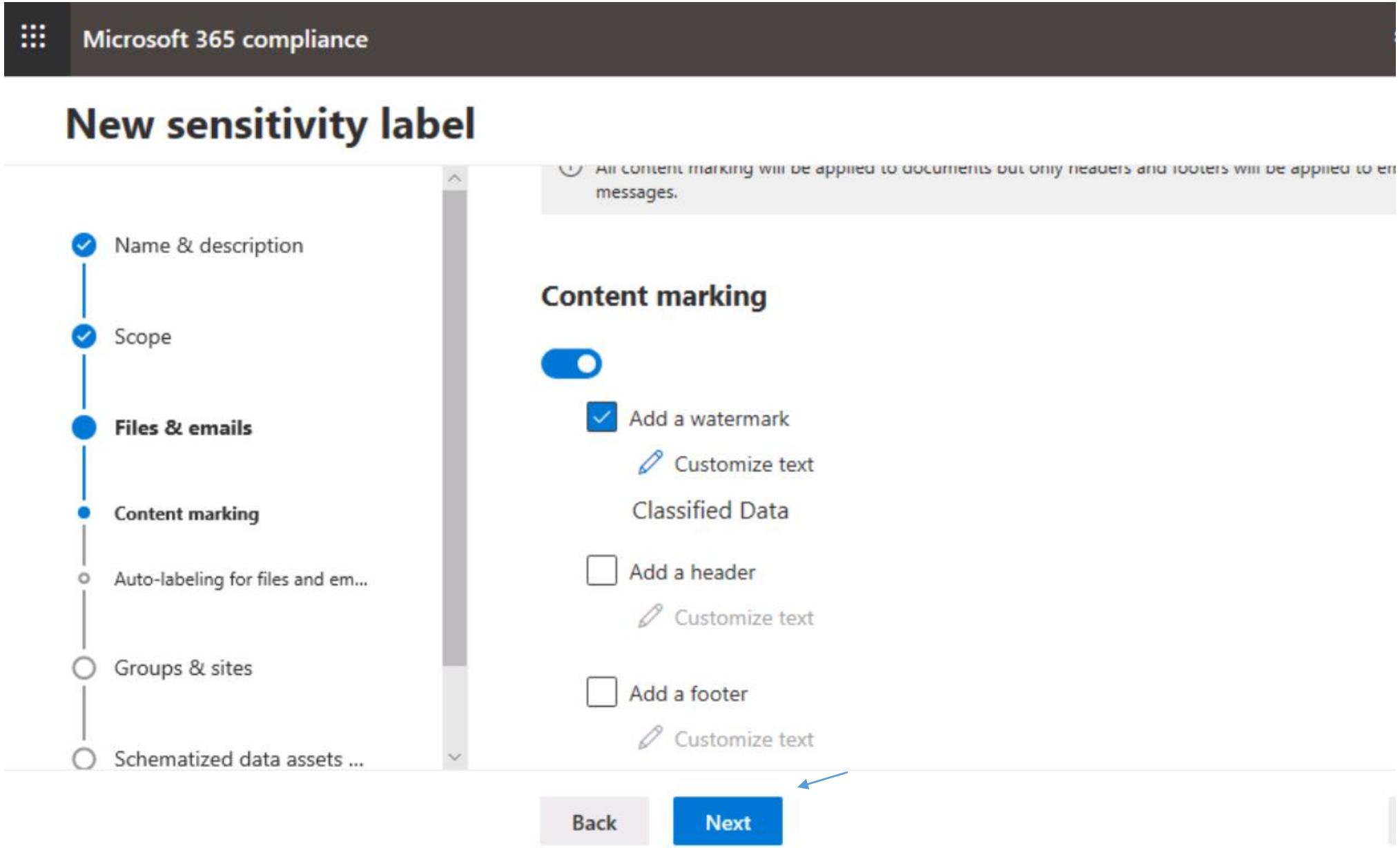

Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Schematized data assets (pr...
Finish
Display name *
Personally Identifiable Information
Description for users *
PII -Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual
Description for admins
PII -Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual
Next
Canc

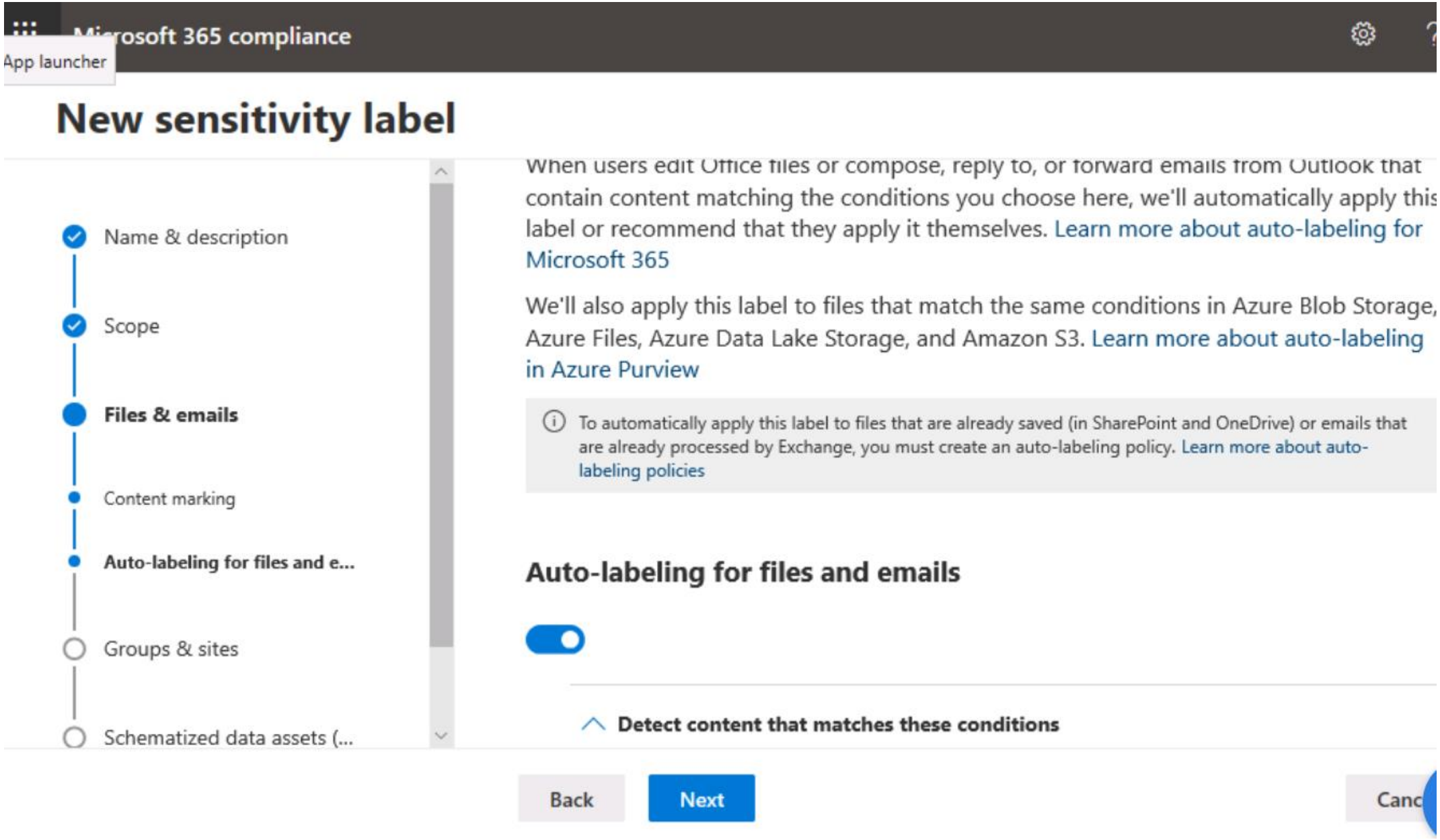

Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Schematized data assets (pr...
Finish
Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes
Files & emails
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.
Groups & sites
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.
To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.
Schematized data assets (preview)
Apply labels to files and schematized data assets in Azure Purview. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.
Back
Next
Canc

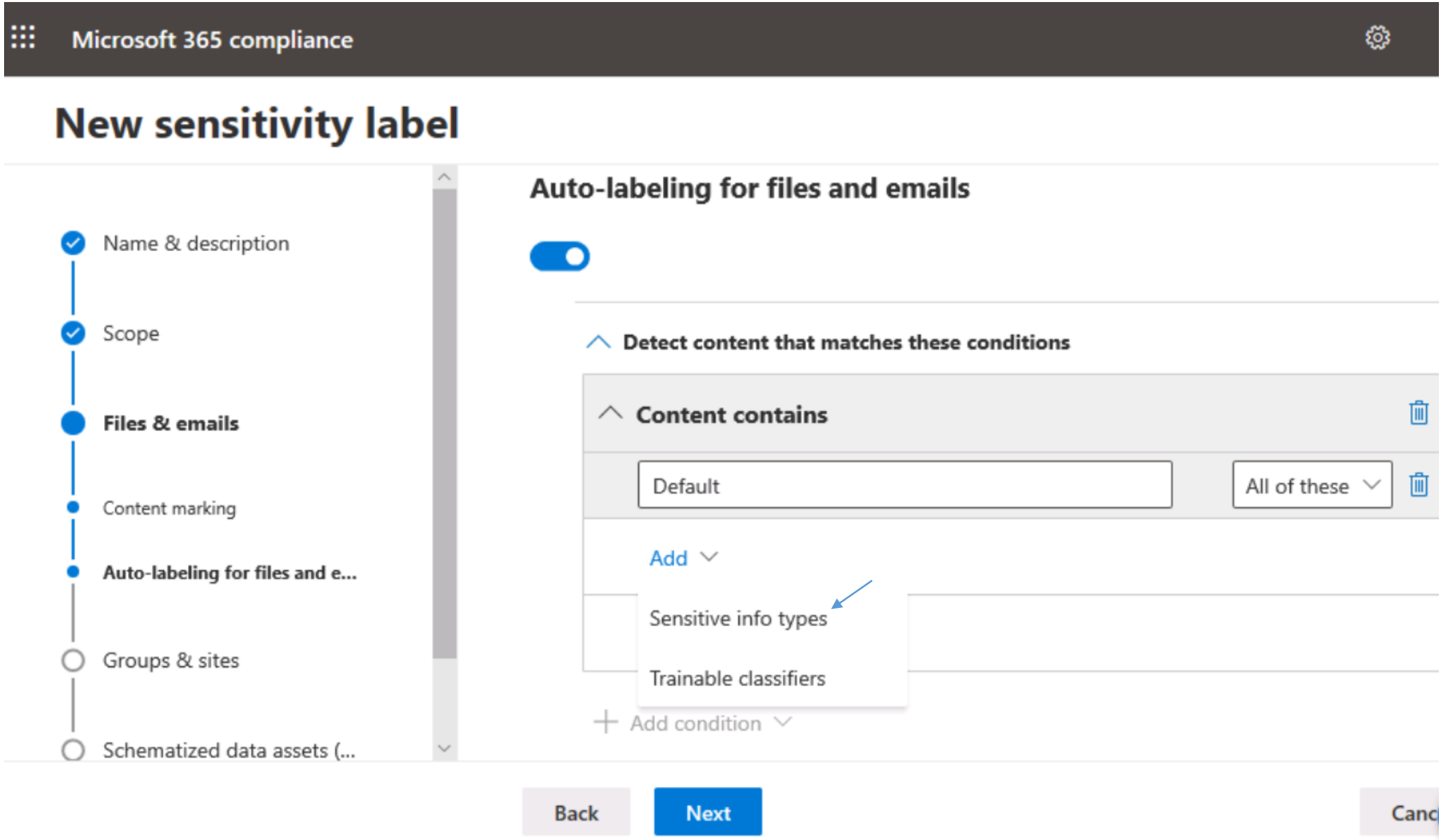

Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Schematized data assets (pr...
Finish
Choose protection settings for files and emails
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.
Encrypt files and emails
Control who can access files and emails that have this label applied.
Mark the content of files
Add custom headers, footers, and watermarks to files and emails that have this label applied.
Back
Next
Canc

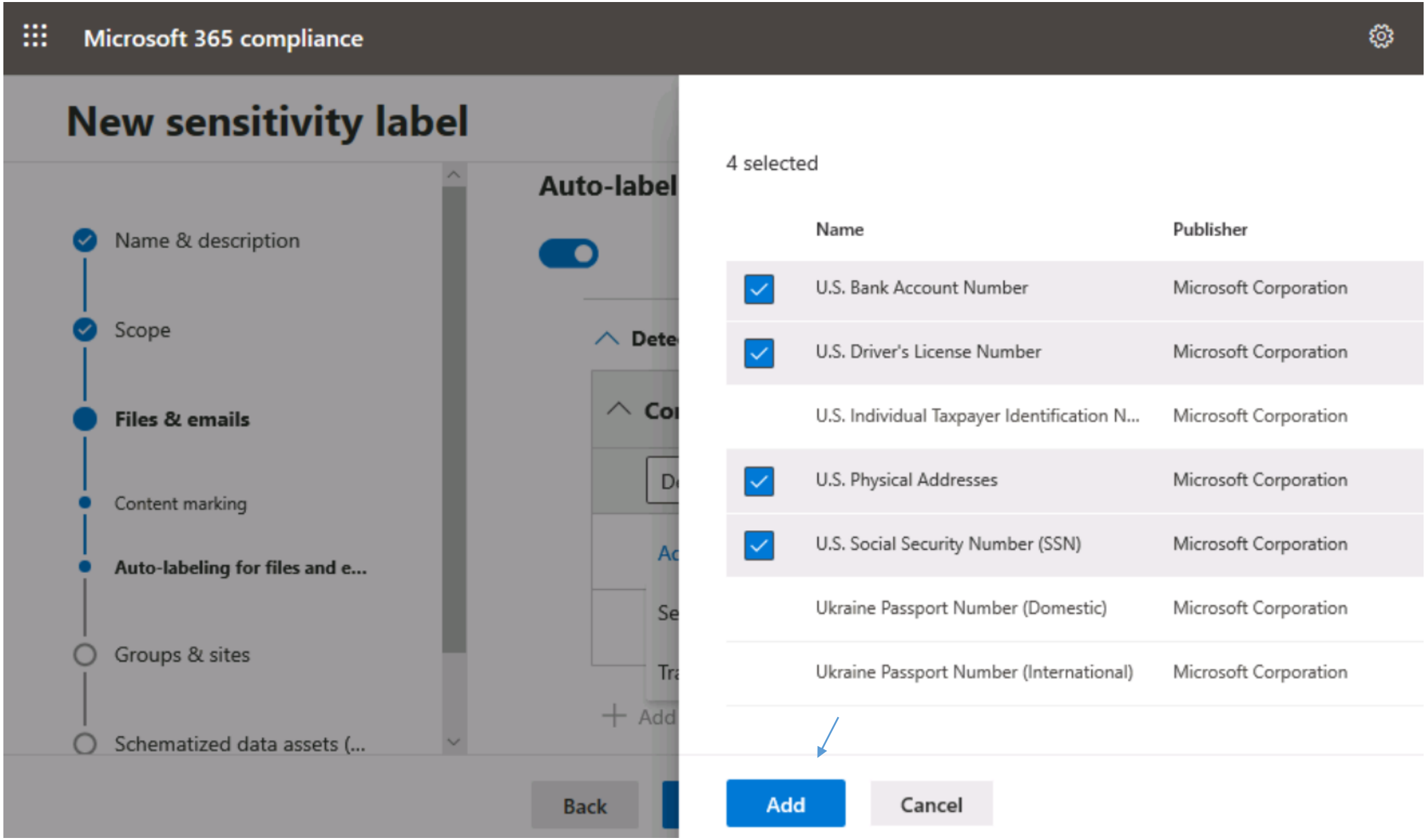

Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and em...
Groups & sites
Schematized data assets ...
Content marking
Add custom headers, footers, and watermarks to content that has this label applied.
Learn more about content marking
All content marking will be applied to documents but only headers and footers will be applied to email messages.
Content marking
Add a watermark
Customize text
Back
Next
Canc

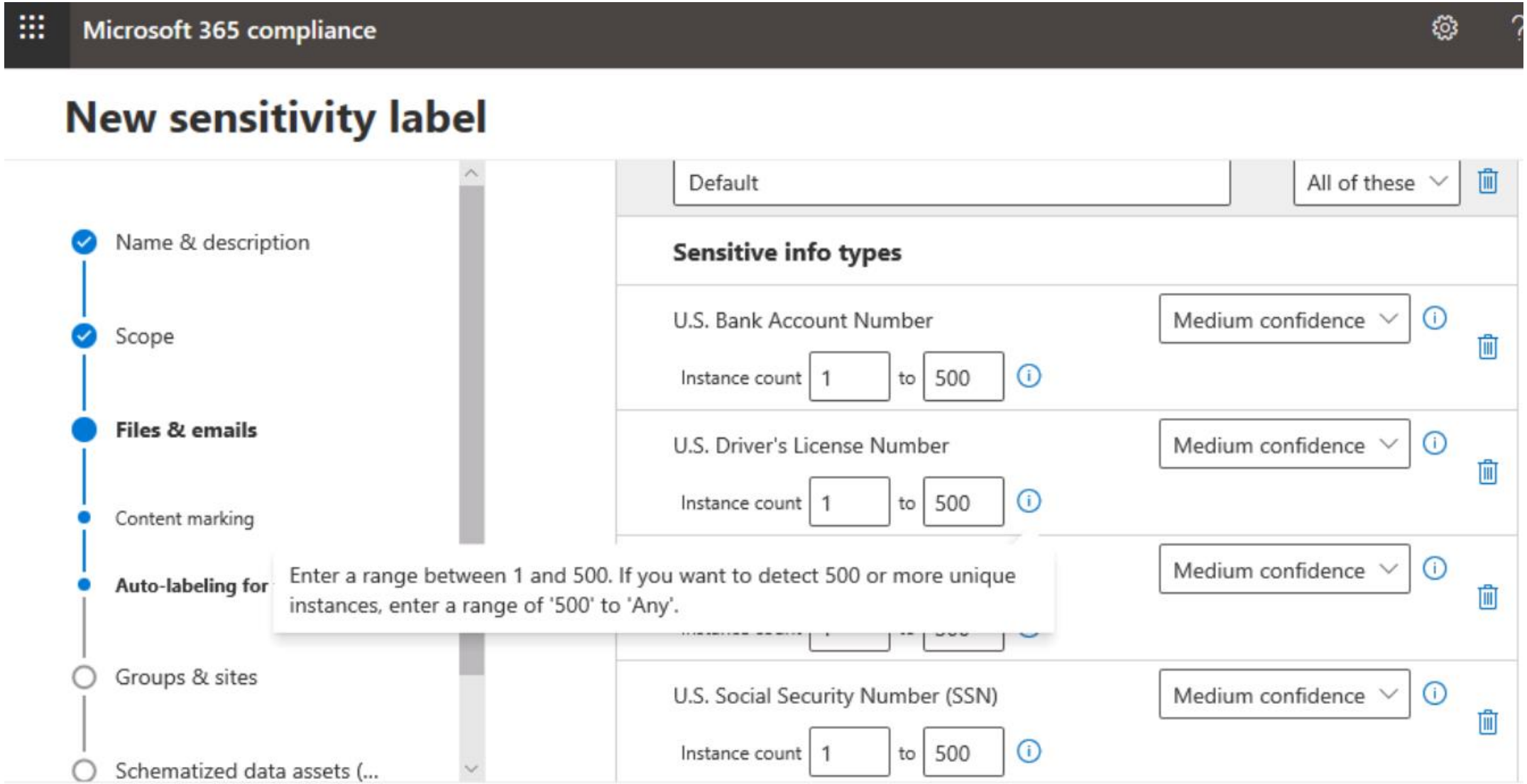

Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and em...
Groups & sites
Schematized data assets ...
Customize watermark text
This text will appear as a watermark only on labeled documents. It won't be applied to email messages.
Watermark text *
Classified Data
Font size
10
Font color
Black
Text layout
Diagonal
Save
Cancel

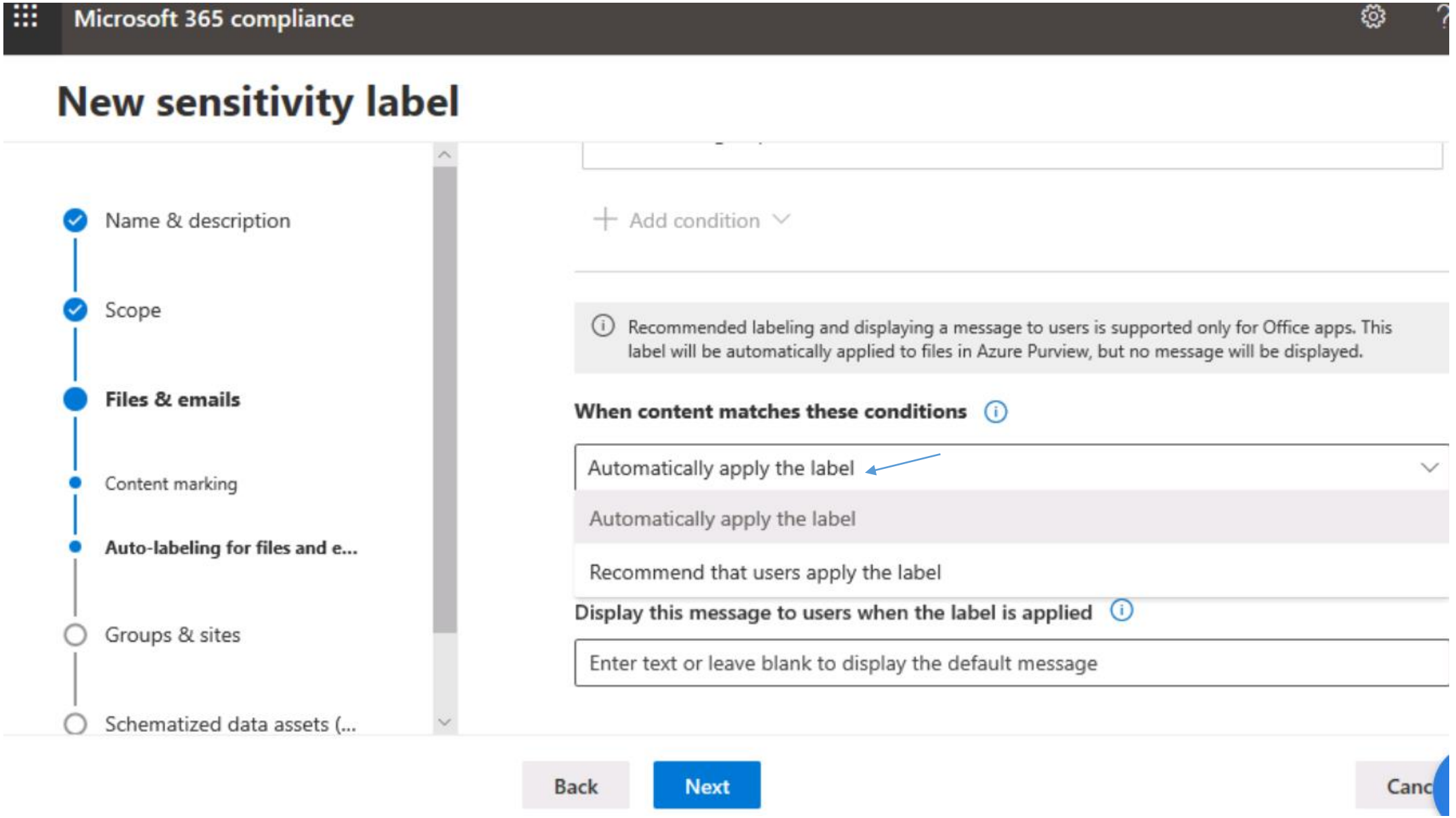

Microsoft 365 compliance
New sensitivity label
messages.
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and em...
Groups & sites
Schematized data assets ...
Content marking
Add a watermark
Customize text
Classified Data
Add a header
Customize text
Add a footer
Customize text
Back
Next

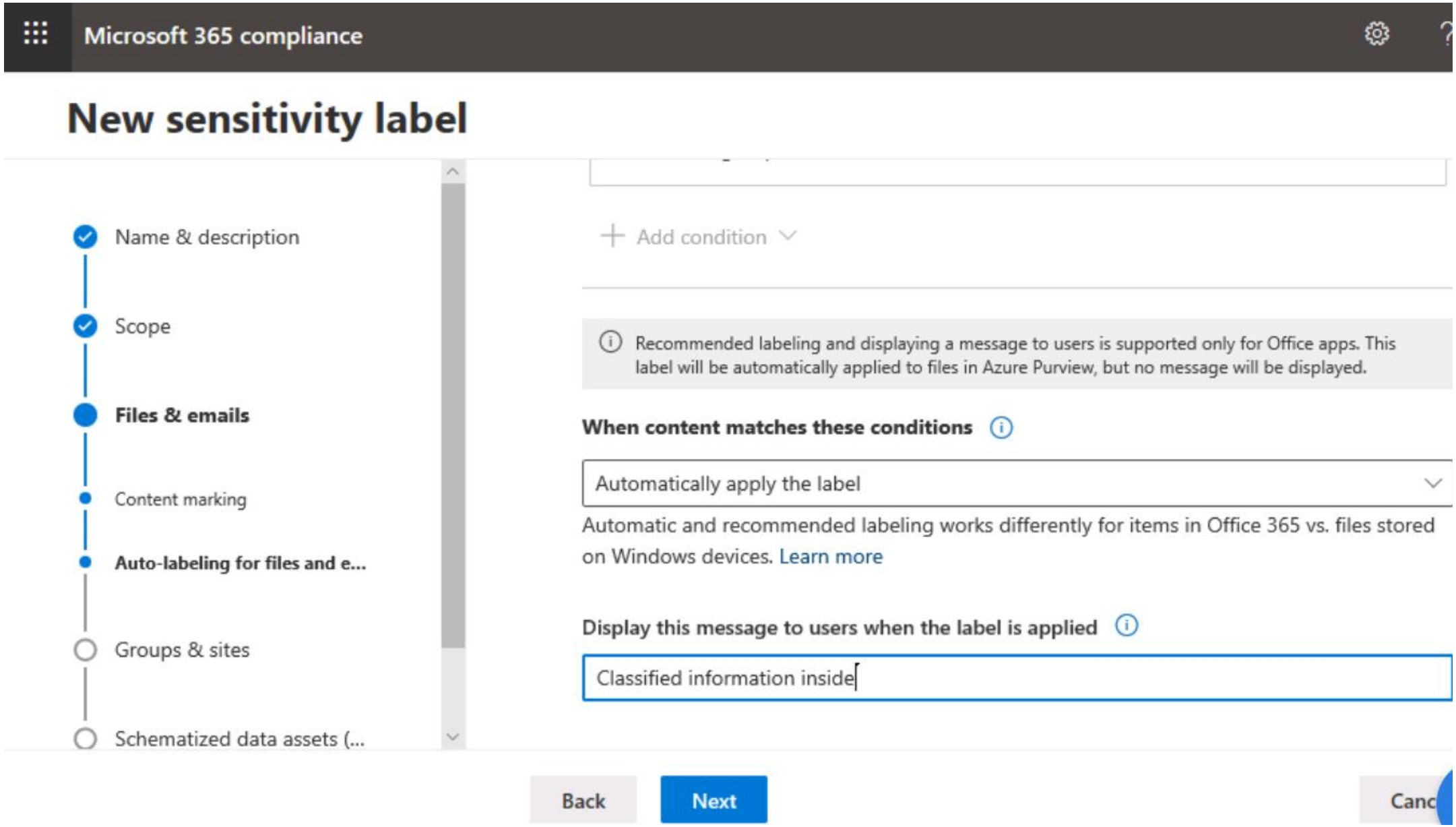

App launcher
Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and e...
Groups & sites
Schematized data assets (...
When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365
We'll also apply this label to files that match the same conditions in Azure Blob Storage, Azure Files, Azure Data Lake Storage, and Amazon S3. Learn more about auto-labeling in Azure Purview
To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies
Auto-labeling for files and emails
Detect content that matches these conditions
Back
Next
Canc


Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and e...
Groups & sites
Schematized data assets (...
Auto-labeling for files and emails
Detect content that matches these conditions
Content contains
Default
All of these
Add
Sensitive info types
Trainable classifiers
Add condition
Back
Next
Canc


Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and e...
Groups & sites
Schematized data assets (...
Auto-label
Back
4 selected
Name
Publisher
U.S. Bank Account Number
Microsoft Corporation
U.S. Driver's License Number
Microsoft Corporation
U.S. Individual Taxpayer Identification N...
Microsoft Corporation
U.S. Physical Addresses
Microsoft Corporation
U.S. Social Security Number (SSN)
Microsoft Corporation
Ukraine Passport Number (Domestic)
Microsoft Corporation
Ukraine Passport Number (International)
Microsoft Corporation
Add
Cancel


Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for
Groups & sites
Schematized data assets (...
Default
All of these
Sensitive info types
U.S. Bank Account Number
Medium confidence
Instance count 1 to 500
U.S. Driver's License Number
Medium confidence
Instance count 1 to 500
Enter a range between 1 and 500. If you want to detect 500 or more unique instances, enter a range of '500' to 'Any'.
Medium confidence
U.S. Social Security Number (SSN)
Medium confidence
Instance count 1 to 500


Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and e...
Groups & sites
Schematized data assets (...
Add condition
Recommended labeling and displaying a message to users is supported only for Office apps. This label will be automatically applied to files in Azure Purview, but no message will be displayed.
When content matches these conditions
Automatically apply the label
Automatically apply the label
Recommend that users apply the label
Display this message to users when the label is applied
Enter text or leave blank to display the default message
Back
Next
Canc


Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Content marking
Auto-labeling for files and e...
Groups & sites
Schematized data assets (...
Add condition
Recommended labeling and displaying a message to users is supported only for Office apps. This label will be automatically applied to files in Azure Purview, but no message will be displayed.
When content matches these conditions
Automatically apply the label
Automatic and recommended labeling works differently for items in Office 365 vs. files stored on Windows devices. Learn more
Display this message to users when the label is applied
Classified information inside
Back
Next
Canc

New sensitivity label

- Name & description
- Scope
- Files & emails
- **Groups & sites**
- Schematized data assets (pr...
- Finish

Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. They don apply directly to the files stored in those containers. Learn more about these settings

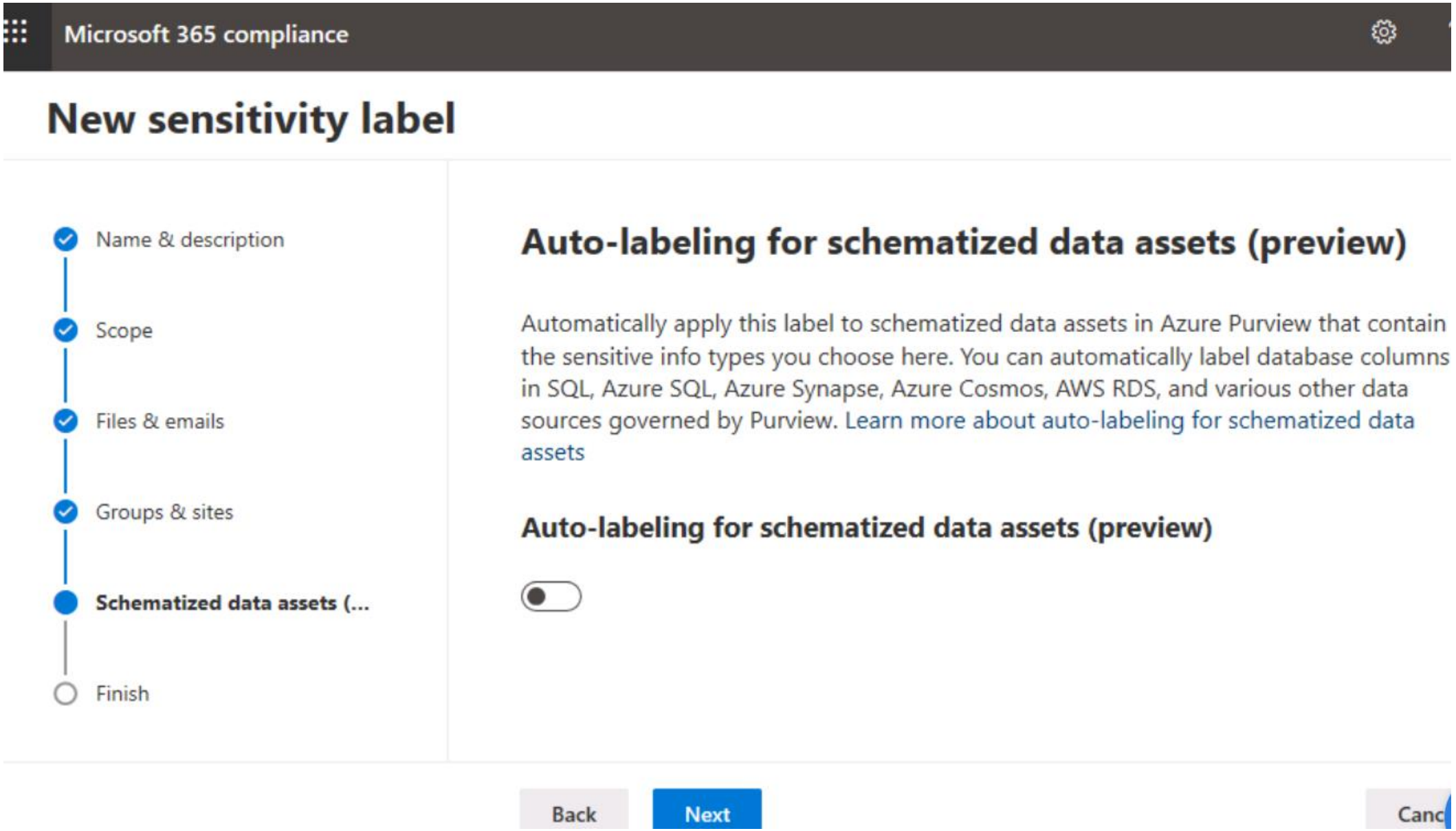
☐ Privacy and external user access settings

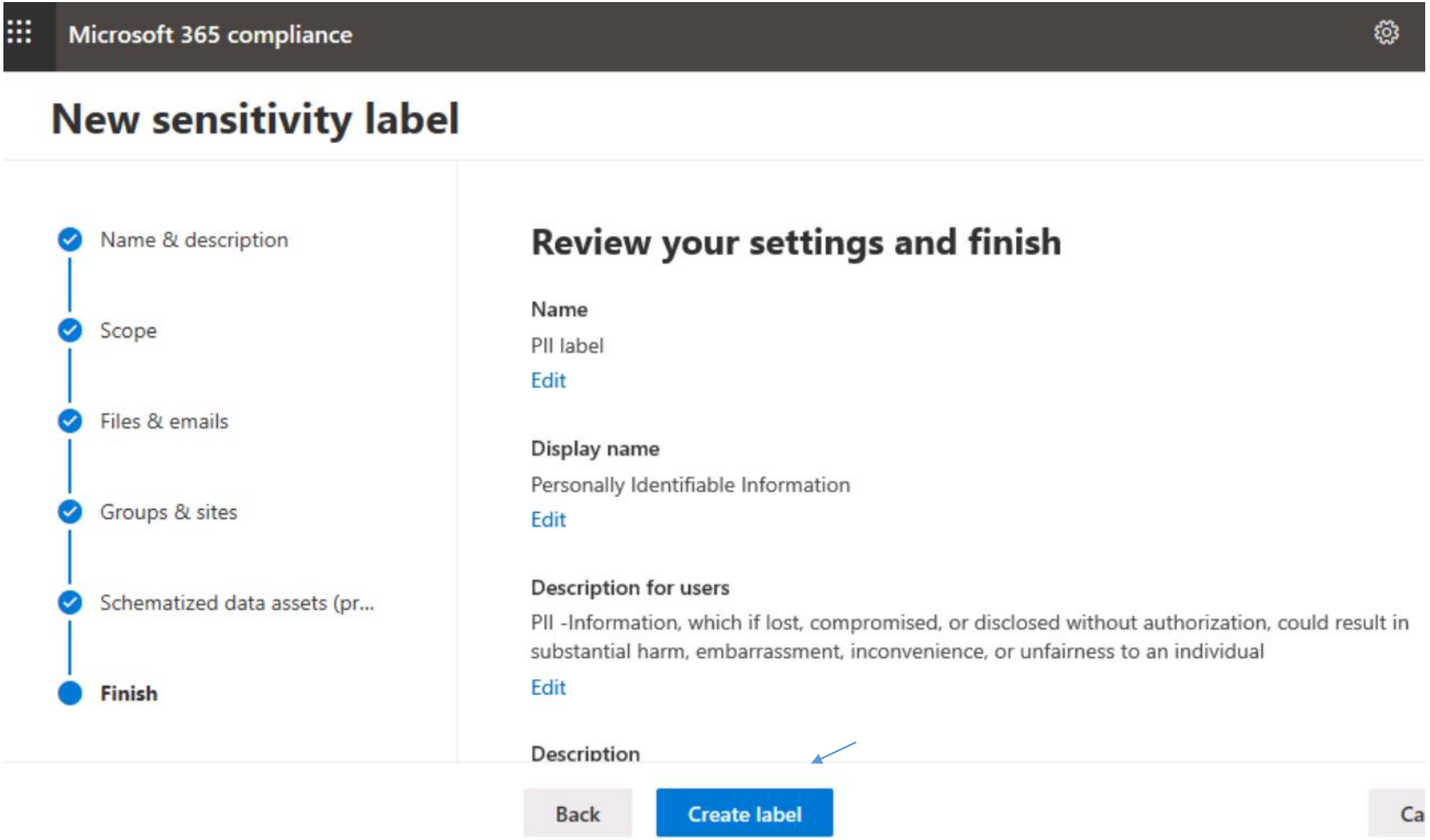
Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

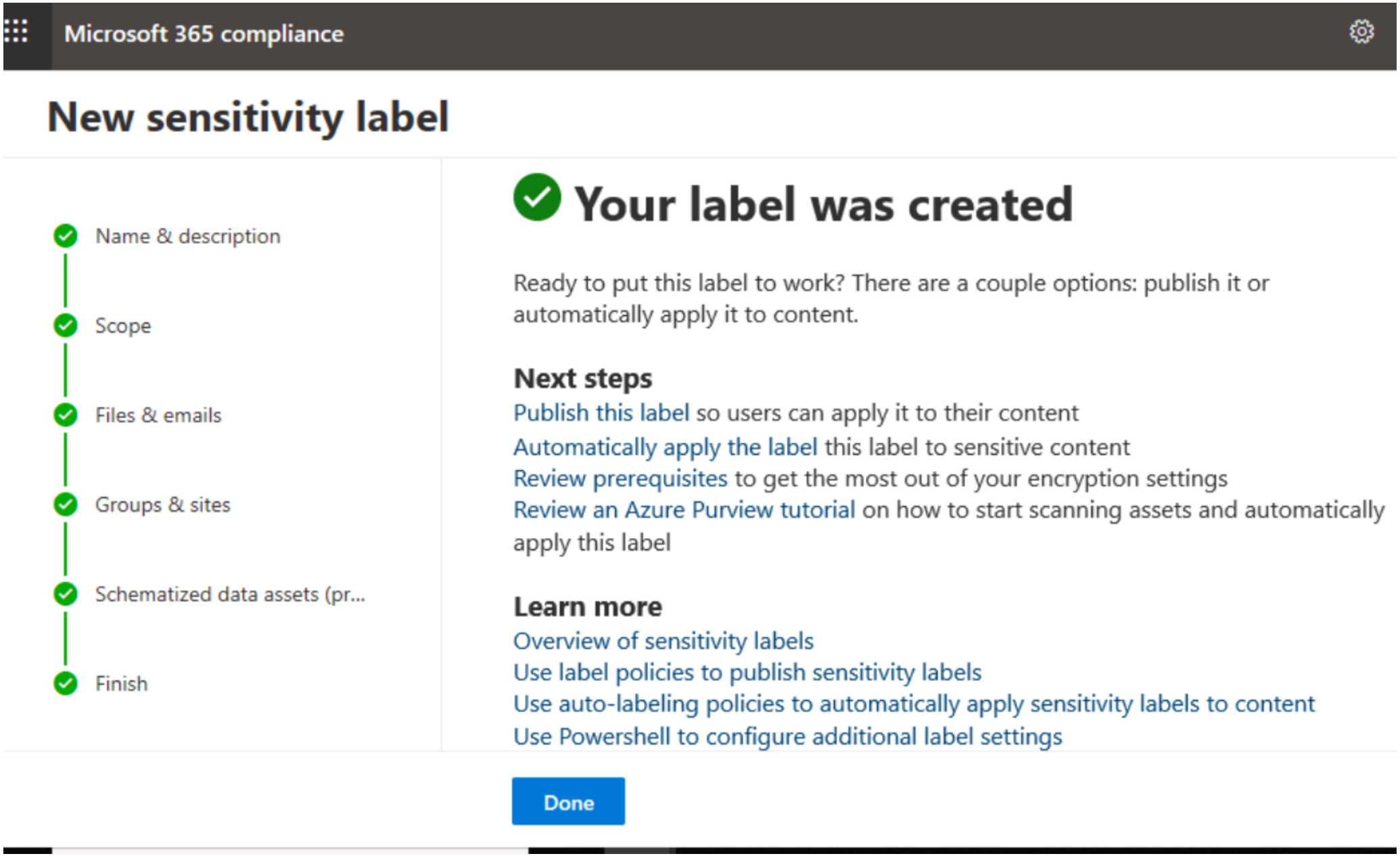
☐ External sharing and Conditional Access settings

Control external sharing and configure Conditional Access settings to protect labeled SharePo sites.

Back | Next | Can

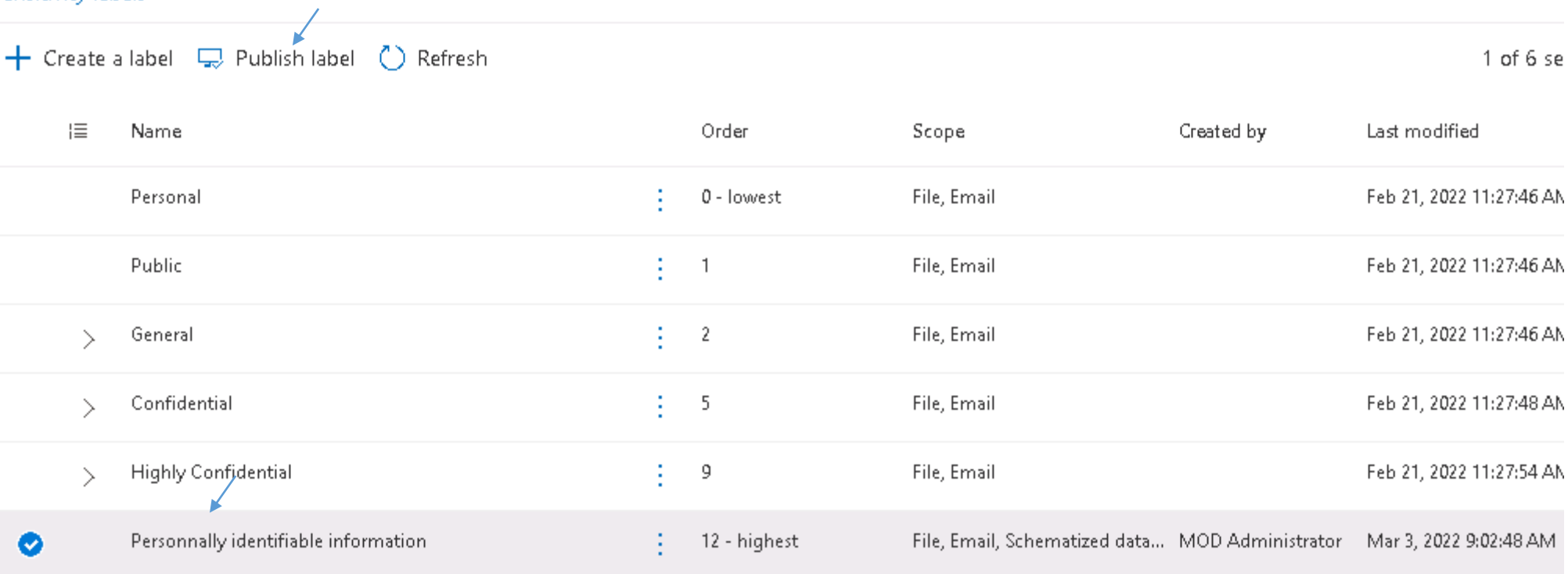

Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Schematized data assets (...
Finish
Auto-labeling for schematized data assets (preview)
Automatically apply this label to schematized data assets in Azure Purview that contain the sensitive info types you choose here. You can automatically label database columns in SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and various other data sources governed by Purview. Learn more about auto-labeling for schematized data assets
Auto-labeling for schematized data assets (preview)
Back
Next
Canc


Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Schematized data assets (pr...
Finish
Review your settings and finish
Name
PII label
Edit
Display name
Personally Identifiable Information
Edit
Description for users
PII -Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual
Edit
Description
Back
Create label
Ca


Microsoft 365 compliance
New sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Schematized data assets (pr...
Finish
Your label was created
Ready to put this label to work? There are a couple options: publish it or automatically apply it to content.
Next steps
Publish this label so users can apply it to their content
Automatically apply the label this label to sensitive content
Review prerequisites to get the most out of your encryption settings
Review an Azure Purview tutorial on how to start scanning assets and automatically apply this label
Learn more
Overview of sensitivity labels
Use label policies to publish sensitivity labels
Use auto-labeling policies to automatically apply sensitivity labels to content
Use Powershell to configure additional label settings
Done

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to e
the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protect based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more ab sensitivity labels



- Labels to publish
- Users and groups
- Settings
- Name
- Finish

Choose sensitivity labels to publish

When published, the labels you choose here will be available in specified users' Office apps (Word, Excel, PowerPoint, and Outlook), SharePoint and Teams sites, and Microsoft 365 Groups.

Sensitivity labels to publish
Personnally identifiable information

Edit

Next

Cancel

Publish to users and groups

The labels you selected will be available for the users, distribution groups, mail-
you choose here.

Location	Included
Users and groups	All Choose user or group

Users and groups

Search

13 items

Name	Email
MOD Administrator	admin@M365x37075546.o...
Alex Wilber	AlexW@M365x37075546.O...
Allan Deyoung	AllanD@M365x37075546.O...
Diego Siciliani	DiegoS@M365x37075546....
Isaiah Langer	IsaiahL@M365x37075546.O...
Joni Sherman	JoniS@M365x37075546.On...
Lynne Robbins	LynneR@M365x37075546....
Megan Bowen	MeganB@M365x37075546.
Microsoft Service Account	ms-serviceaccount@M365.

Done Cancel

- Labels to publish
- **Users and groups**
- Settings
- Name
- Finish

Publish to users and groups

The labels you selected will be available for the users, distribution groups, mail-enabled sec
you choose here.

Location	Included
Users and groups	1 user or group Choose user or group

Back Next

- Labels to publish
- Users and groups
- **Settings**
- Name
- Finish

Policy settings

Configure settings for the labels included in this policy.

Users must provide a justification to remove a label or lower its classification

Users will need to provide a justification before removing a label or replacing it with one that has a lower-order number. You can use activity explo to review label changes and justification text.

Require users to apply a label to their emails and documents

Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already h label applied).

ⓘ Support and behavior for this setting varies across apps and platforms. Learn more

Require users to apply a label to their Power BI content

Users will be required to apply labels to unlabeled content they create or edit in Power BI. Learn more about mandatory labeling in Power BI

Provide users with a link to a custom help page

If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. Learn more about this help pag

Back Next

- Labels to publish
- Users and groups
- **Settings**
- **Documents**
- Emails
- Power BI
- Name
- Finish

Apply a default label to documents

The label you choose will automatically be applied to Word, Excel, and PowerPoint documents when they're created or modified. Users can always select a different label to better match the sensitivity of their document. Which Office app versions support this setting?

Apply this default label to documents

Personnally identifiable information

Labels to publish
Users and groups
Settings
Documents
Emails
Power BI
Name
Finish

Apply a default label to emails

The label you choose will automatically be applied to new and existing, unlabeled emails. Users can always change the default label before they send the message. If you selected the 'Require users to apply a label to their email messages and documents' option earlier, you can turn that requirement off for emails here. Which Outlook versions support these settings?

Apply this default label to emails

Personnally identifiable information

Require users to apply a label to their emails

Back Next Cancel

- Labels to publish
- Users and groups
- **Settings**
- Documents
- Emails
- **Power BI**
- Name
- Finish

Apply a default label to Power BI content (preview)

The label you choose will automatically be applied to new Power BI reports, dashboards, and datasets. Users can always change the default label if it's not the right one. Learn more about mandatory labeling in Power BI

Apply this default label to Power BI content

None

Back Next Cancel

- Labels to publish
- Users and groups
- Settings
- **Name**
- Finish

Name your policy

Name *

policy for PPI

Enter a description for your sensitivity label policy

Personally Identifiable data policy

Back Next

App launcher

bel policy > Create policy

- Labels to publish
- Users and groups
- Settings
- Name
- **Finish**

Review and finish

Name

policy for PPI

Edit

Description

Personally Identifiable data policy

Edit

Publish these labels

Personnally identifiable information

Edit

Publish to users and groups

AlexW@M365x37075546.OnMicrosoft.com

Edit

Policy settings

Label is mandatory for: documents, emails
Default label for documents is: Personnally identifiable information
Default label for emails is: Personnally identifiable information
Users must provide justification to remove a label or lower its classification

Back

Submit

- Labels to publish
- Users and groups
- Settings
- Name
- Finish

New policy created

It can take up to 24 hours to publish the labels to the selected users' apps.

Next steps

Review data classification reports to see how labels are being used

Read guidance on how to educate users about sensitivity labels

Done