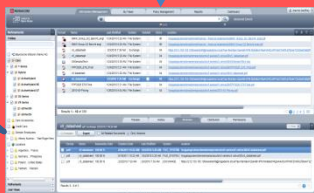


## Analyze, organize and clean up all data

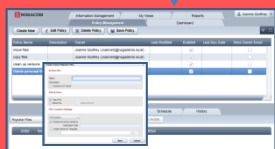
Check the dashboard for a snapshot of the data



Go to the UI for more specific details



If needed, check the reports for further information

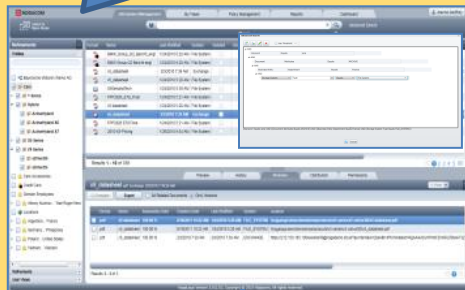


Take initial action to organize and clean up data stores:

- Archive old data
- Delete unnecessary copies
- Reorganize storage locations
- Move versions
- Remove personal data
- Remove audio and image files

## Identify and organize sensitive data

Identify sensitive data based on business context, through the UI (enhance results using keywords, properties, regular expressions, file formats, date modified, author, repository etc.)



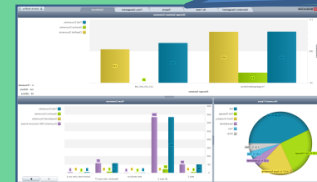
Name	Description	Date
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101
101-101-101	101-101-101	101-101-101

Organize different types of sensitive data into relevant 'Views' based on business and regulatory requirements.

Add tags to select documents such as: Public; Non-Confidential Business Information; Sensitivity Undetermined ; Confidential Business Information ; Data Leak Prevention

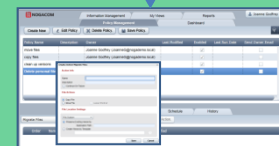
## Discover, analyze and resolve problems

Check the dashboard to get a snap shot of each 'View' to prioritize problem areas to focus on.



Drill down through the reports to get detailed information on each 'View' including:

- Access rights
- Audit history
- Storage locations
- Copies & versions
- Email distribution



Take action to address problems and effectively protect and govern sensitive data:

- Manage copies and versions
- Move files to protected repositories
- Change/update access rights
- Update business practices
- Re-educate end-users
- Export to DLP and other technologies