File Access Manager

Data Privacy

Version: 8.3 Revised: March 29, 2022

Contents

DSAR Background

Due to an increasing awareness for privacy, regulators have been led to introduce new Data Privacy and Data Protection requirements in order to protect consumer, health, financial and other sensitive information.

In recent years as data has become digitized, more prevalent, and more accessible, these laws and regulations are stricter and are being passed more frequently. These laws are passed with the objective of giving control back to individuals over their personal data. However, the Privacy Regulation landscape is becoming more and more complex and compliance is becoming more and more of a challenge.

Recent regulations inspired by the long-standing GDPR Data Privacy and Protection Regulation, require organizations to identify and detect personal identifiable information (PII) such as Name, Aliases, Addresses / Locations, SSNs, IDs, email addresses, account numbers, etc. Organizations need be able to respond and disclose all occurrence of a person's PII data upon request.

These requests, often referred to as the Right-of-Access and the Right-to-be-Forgotten, are handled by processes called Data Subject Access Requests (DSARs). Also known as a "subject rights request" or a "privacy rights request," a DSAR is a submission by an individual (or data subject) to a business asking to know what personal information of theirs has been collected and stored, as well as how it's being used.

Individuals can also use a DSAR to ask that the company take certain actions with their data, such as deleting it, fixing incorrect data, or opting out of future data collection. Enterprises worldwide are faced with the task of responding to these and thousands of similar privacy requests annually – all of which must be completed within strict time frames. Yet, the current processes to do so are both time-consuming and complicated.

There are several clear and distinct steps that most DSARs go through. The biggest hurdle for organizations is the data discovery process – locating individual identity information within huge volumes of unstructured data. Another key challenge is coordinating within the organization between the different stakeholders that need to be involved in correlating, validating and remediating the detected information. Verifying that the remediation was successful and orchestrating and managing compliant responses to requesters and auditors are other tasks that need to be completed. This is especially difficult, as current processes used to identify, correlate, and remediate the data, as well as manage compliance responses, are primarily manual, prone to errors, and aren't scalable.

File Access Manager Privacy Engine includes the DSAR Campaign Workflows capability. This means automated DSAR campaign workflows that leverage AI-Driven NLP-based data discovery and orchestrates data validation, remediation and verification reviews, to address complex compliance requirements, enable quick collaboration, and considerably cut processing time - enabling organizations to scan, identify, report on and collaborate over the remediation of Personally Identifiable Information.

DSAR Workflow

Processing DSARs include several stages.

- Submitting the request – An individual submits a request for information to be disclosed, removed, or edited
- Validating the identity – The organization receiving the request must validate the requester identity. This is done to ensure the request is valid and that the information is disclosed only to that particular individual or an authorized proxy
- Discovering the data – Typically the longest stage. All PII information associated with the individual across all of the organization data sources is identified

- Validating the data – Once all PII information is discovered, the data that was found will need to be validated to ensure that it does in fact relate to the data subject
- Remediating the data – If the requester asked for data to be redacted, updated or removed, this stage will address those requests.
- Verifying – Once remediation is complete, ensure the data detected was modified or removed
- Responding – As part of the DSAR response, all data about the individual and the processing it went through are reported, packaged and securely delivered to the requester

File Access Manager DSAR campaign workflows address the Data Discovery, Validation, Remediation and Verification stages. Once data is discovered by the privacy engine, each campaign workflow is comprised of these steps:

Phase One – Data Validation

In this phase, the reviewer is presented with the results found based on the campaign DSAR query and scope. The reviewer must review the identified files. Reviewers must decide whether the files found should be included in the DSAR processing, or should be excluded from further processing. A reason a file could be excluded might be due to a file being detected by mistake.

All decisions made should be committed in order to complete the review level.

The review process can involve multiple reviewers at each stage. However, a decision on each file can only be made by a single reviewer.

When all the results have been excluded or confirmed and committed, the campaign will transition to the data remediation phase. Campaigns transitioning to the Data Remediation phase will see their status change to "Data Remediation in Progress". The status of the campaign may take a few moments to be updated.

Phase Two – Data Remediation

The data remediation phase will include all files confirmed for further processing. In this stage, reviewers will collaborate by reporting the completion of the remediation task, such as redacting or removing the PII data, or exclude the files from remediation (due to contesting compliance requirement, e.g.).

After files have been reviewed and acted on, the reviewer must either mark the files that have been acted on as Done or mark data that cannot be acted on as Excluded.

When all files are marked as Excluded / Done and everything has been committed, the workflow service will change the DSAR campaign's status to Data Remediation - Completed.

> The status of the campaign may take a few moments to be updated.

Phase Three – Data Verification

The purpose of the Data Verification phase is to verify that the remediation actions have been performed correctly and that all detected information has been addressed (whether it's removed, redacted or changed).

Once verification has been initiated:

a. A task will be created. Wait until it is finished (this can take awhile)

b. The campaign status will change to Verification in Progress

When the task is finished, the campaign status will change to Verification is Done.

> If the verification task failed, the campaign status will change to Verification Failed.

To view the campaign verification results, navigate to **Compliance > DSAR Management > DSAR Campaign Details**.

a. If the requested campaign query yields results on a file, it will be marked as Failed.

b. If the requested campaign does not yield results on file, it will be marked as Verified.

c. If the requested campaign yields results but with exceptions, it will be marked as Verified with Exceptions.

d. If the file is not accessible or if the file does not exist, it will be marked as Unable to Verify.

In this phase, the administrator or compliance manager can decide to override a failed campaign, reassign it to another reviewer, or force it back into the remediation phase.

Campaign Details

DSAR Campaign Purposes

Each DSAR Campaign has a Purpose field, indicating the purpose for which the requester submitted the request. The different type of request purposes determine the workflow stages involved and its final outcome.

- **Information Disclosure** – Designed to find the relevant personal information regarding the individual based on the search criteria set in the DSAR campaign definition. Information Disclosure DSARs include a single phase review process (a Data Validation Phase), unlike all other DSAR types that include a two-phased review process. Once the Validation phase is completed, the Campaign will transition to a Completed status.
- **Data Redaction (Editing)** – Designed to find the relevant personal information that needs to be redacted based on the search criteria set in the DSAR campaign definition. Data Redaction includes a two phase process (Data Validation [phase one] and Data Remediation [phase two]). Once committed, the DSAR goes to Verification Phase.
- **Data Deletion** – Designed to find the relevant personal information that needs to be deleted based on the search criteria set in the DSAR campaign definition. Data Deletion includes a two phase process (Data Validation [phase one] and Data Remediation [phase two]). Once committed, the DSAR goes to Verification Phase.

Campaign Due Date

Each DSAR Campaign has a deadline or a date in which a response is due. When setting up a campaign, the due date can either be a set date, or a period of time after the campaign is started.

DSAR Query

This defines the DSAR search criteria to identify the data on which to perform the actions. This includes PII information data points such as Identifiers, Names and Aliases, Addresses, Emails, and more. Each field can be mandatory or optional in your search.

Supported Applications

Data Classification supports the following applications:

Target System	Products and Supported Versions
On-premises File Storage	Microsoft Windows
	Microsoft SharePoint
	NFS v3/v4
NAS File Storage	NetApp for CIFS
	NetApp for NFS
	EMC Celerra/VNX/Unity for CIFS
	EMC Celerra/VNX for NFS
	EMC Isilon for CIFS
	Hitachi HNAS
	DFS for CIFS
	Generic CIFS
O365 File Storage	Microsoft OneDrive for Business
	Microsoft SharePoint Online (Office 365)
Cloud File Storage	Box
	Dropbox
	Google Drive
	Ctera
	Azure Files

Supported File Types

The privacy engine indexes data, based on a file's content and attributes. The system also supports file properties and custom properties for all supported file types. The privacy engine reads file content, based on the file extension.

Image files can be analyzed and searched for keywords using an optical character recognition (OCR) capability in . This is a resource heavy process, and is configured separately. See section Optical Character Recognition (OCR).

The Data Classification engine supports the following file types /extensions:

File Extension	Expected file type
docx doc xls xlsx ppt pptx	Microsoft Office files
txt csv	Plain Text (including Comma Separated Values files)

File Extension	Expected file type
htm html xml	Web files
cs js sql	Code script files
pdf	
zip gzip tar rar 7zip	Archive files
Jpeg jpg tif tiff gif png wmf emf bmp pdf	Image files analyzed by the OCR module*

The system downloads files from cloud-based content stores and non-CIFS application (for example, Box, DropBox, Google Drive, OneDrive, SharePoint and NFS) to a local directory on the server. Once the indexing process finishes, the system deletes the downloaded files from the indexing server.

Optical Character Recognition (OCR)

File Access Manager can identify text from within image files either directly, or embedded in other files – such as a scanned driver's license image attached to an MS Word document, or a collection of scans stored in a zip file. Files less than 1000 pixels across will not be scanned, to avoid less reliable results from low resolution images.

The data privacy engine can analyze files containing sensitive data in image form.

> The optical character recognition process is resource intensive, and should be configured carefully taking the runtime into consideration. It is disabled by default.

OCR Capability can be added to the scope selected in the DSAR Scope screen.

Enabling Optical Character Recognition

By default, optical character recognition is disabled on the entire scope of the DSAR. To enable optical character recognition on a resource, edit the application scope line.

1. Find the desired application from the DSAR Scope screen.
2. Click **Edit**.
3. Click **Optical Character Recognition (OCR)** to enable OCR analysis for this application.

Privacy PII Detection Architecture and Flow

The File Access Management Data Privacy feature is powered by SpaCy (an open-source library for advanced natural language processing textual analysis). Using the SpaCy AI model, File Access Management can detect names and addresses using contextual analysis of the scanned documents' contents.

Text PII Detection

File Access Management uses various tools to detect PII:

- Name and Address – using the SpaCy NER module (named entity recognition) with SailPoint custom trained model allows the detection of both name and address
- Identifications (Social Security Numbers, employee ID number, etc.) – File Access Management will use regular expressions to identify IDs
- Emails – File Access Management uses the SpaCy built-in email regular expression pattern
- Phone Numbers – File Access Management uses the SpaCy pattern matching feature to detect phone numbers based on predefined formats

  File Access Manager's Privacy PII detection engine will attempt to match both local and international phone number patterns if they comply with the standard format of the relevant country.

Supported Formats	Unsupported Formats
+1.253.215.8782	1300030886
(212) 465-6471	22.4389483
(212) 465-6471	

PII Search and Relevancy Scoring

The File Access Manager Privacy Engine will search for all submitted PII search criteria.

Search criteria marked as "Required", will be mandatory. If a file does not match these criteria, it will not be returned as a result.

Search criteria that are not marked as "Required" will not exclude a file if not matched, but will contribute to the overall relevancy score.

Relevancy Score

A document relevancy score signifies the proximity between the document content and the search criteria.

The higher the relevancy score, the higher the probability the information matched belongs to the individual whose details we've entered in the search criteria.

The more elaborate and well-defined the search criteria is, the better accuracy the privacy engine can produce. For example, searching for just a first name or a nick-name is likely to return a large number of false positive, since there are likely to be many matches of that name.

However, searching for a specific email, name, and ID is likely to produce much more accurate results.

The relevancy score is calculated based on the number of search criteria and the accuracy of the data the privacy engine was able to match.

Each search criteria has a relative relevancy score allocation that contributes to the overall relevancy score.

For example, when you perform a search using four search criteria, each criterion has a weight of 25% of the overall score, or a relative score accounting for 25% of the overall score.

The overall score will be based on the number of criteria matched. If the search matched only one out of four search criteria, the overall relevancy score would be 25%.

If two search criteria were matched, the relevancy score would be 50%, and so forth. A full match of all search criteria would yield a 100% relevancy score match.

Name fields offer more granular relevancy scoring. If a name search criteria is matched in its entirey, then it will contribute the full amount of its relative relevancy score.

However, Name fields (the Name and Alias fields) are also evaluated for partial matching. In case a name search criteria was partially matched, it will contribute only 50% of it's relative relevancy score to the overall score.

For example, with a four-term search criteria, when one of the search criterion is the name "John Smith", the name field will have a 25% relative relevancy score.

If the name is matched fully, that is, the name "John Smith" in matched fully in the document, the name search criteria will contribute the full 25% to the overall relevancy score.

However, if the name is partially matched, for example, the file contains "John" or "Smith", only half of the relative relevancy score would be accounted for in the document overall relevancy score.

Thus, the more search criteria involved in the DSAR query, the less impact partial matching have on the overall score, since the likelihood that the identity search for was actually matched is much higher.

So, in the previous example, if we're looking for 4 data points (e.g., ID, Address, Email and Name) - the search matched the first three and fully matched the name - the relevancy score would be 100%.

However, if the first three criteria are matched and the name is matched partially, the relevancy score would be 87%. It is still high, since we hit 4 different data points and there's a high probability the document matched the identity, or individual we're searching for, even if the name was not fully matched. However, if the query is searching just for a name, and the name is partially matched, then the overall score would be 50%, as opposed to a 100% for a fully matched name.

Lower probability documents are documents with a low relevancy score. They can easily be excluded from further DSAR processing. The decision to exclude files from further DSAR processing is with the discretion of Privacy Manager and Reviewers.

DSAR Management Screen

The DSAR Management Screen allows Compliance Administrators to create, manage, and track DSAR Campaigns, monitor their progress, perform actions, and view their current status.

Using this screen, the user can create the DSAR campaign, follow the statuses of validating and remediating the data, and also perform data verification.

To open the DSAR Management screen navigate to **Compliance > DSAR > DSAR Management**.

To add or remove columns from the grid, click the column chooser icon. Next click **List More** and check / uncheck the required columns.

Name

Name of the DSAR campaign

Purpose

Reason for the DSAR campaign

Current Status

The campaign statuses can be one of the following:

- Data Discovery
- Data Validation
- Remediation - In Progress
- Remediation - Completed
- Verification - In Progress
- Verification - Completed
- Completed
- Failed
- Pending Deletion
- Pending Cancel
- Cancel

Due Date

The DSAR campaign deadline (date).

Creation Date

Date the campaign was created.

Actions

- Edit - Opens the Wizard in Edit mode

> When editing a campaign, if the campaign hasn't been executed yet, all the campaign's settings and attributes can be edited. However, if the campaign was already executed, only the campaigns general details can be updated. The DSAR Query and the Review Process settings cannot be changed at this stage. For more information, view Creating a DSAR Campaign

- Generate Report - Generate the campaign report

Description

General information about the campaign

Owner

User who created the campaign

Start Date

Date the campaign is set to start

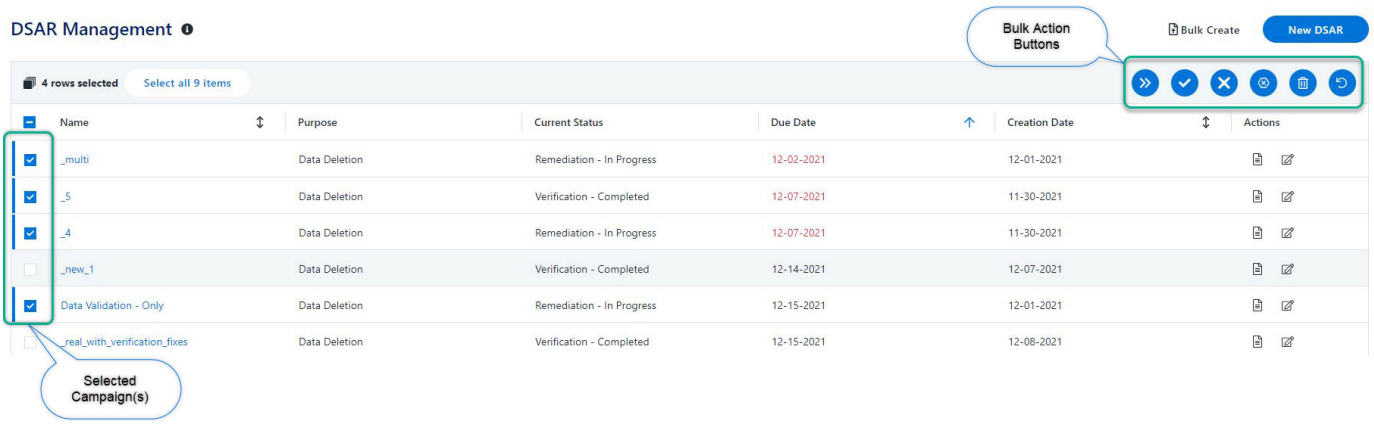
End Date

Date the campaign is set to end

Duration

The amount of time the campaign is Active. The number of days between the Start Date and the End Date.

If no End Date is available, then the current date is used for calculations.



Selecting campaigns for bulk

Select campaigns by clicking the checkbox in the left column.

This will open a multiple-select option on the top of the grid: **Select all [X] Items**.

Editing an active campaign

Click the **Edit** icon on the campaign row.

Once a campaign has been saved and ran, a user can only edit the campaign name, description, review instructions, due date. The Reminder Schedule can also be edited on the Summary page.

- Changing any of the due date fields will recalculate the remaining fields according to the new configuration.
- Switching from a specific date to a time period, for example 2 weeks, will clear the due date field.
- If the campaign has already started, the due date will be recalculated from the start date and time period.

Editing a campaign that is not active

Click the **Edit** icon on the campaign row.

If a campaign has been created but not ran, a user can edit all settings in the campaign.

Running a report based on a campaign

Click the **Generate Report** icon on the campaign row. For more information on Reports, see DSAR Reports.

To run one or more campaigns

Select the campaigns in the left hand boxes, and click **Run Campaigns**.

All inactive campaigns (campaigns that have not run yet) will start running. The due date of these campaigns will be calculated at this time.

To verify one or more campaigns

Select the campaigns on the left check boxes, and click **Verify Campaigns**.

This action is available after the campaign reaches “Remediation - Completed” status, and until it reaches the “Completed” status.

The Verify action triggers a verification task that rescans the results found during the discovery task and verifies the successful remediation of these records meaning that the information no longer exists.

To cancel one or more campaigns

Select the campaign to cancel.

To end one or more campaigns

Select the campaign to mark it as 'Complete' despite not having a completed campaign.

To delete one or more campaigns

Select the campaigns on the left hand tick boxes, and click **Delete Campaigns**.

Filters

To filter the results on the grid, click the filter icon on the heading bar. Select the requested criteria.

> The default filter setting is set to show Active campaigns.

Click **Apply** to apply the filter, or **Clear All** to clear the filter and repopulate the grid.

> Make sure no campaigns are selected in order to be able to access the filter icon

Name

Enter all or part of the campaign name

Current Status

Search by status of the campaign

Purpose

Search by entering any of the campaign purposes

Owner

Search by the user who created the DSAR campaign

Due Date

Select the date type, and date / range. Use the date chooser to select dates.

- Equals - Enter the due date
- Last X days - Enter the number of days back to select
- Next X days - Enter the number of days forward to select
- Between - Enter the date range. Open the date chooser, click the start date, then click the end date.

Creation Date

Search by selecting the known date

Start Date

If the campaign start date is set, search by selecting the start date

End Date

If the campaign end date is set, search by selecting the end date

Pre-defined Filters

The buttons on the top-left corner of the DSAR Management screen's grid are pre-defined filters. See image above. When clicked, these filters override existing filters.

View All

Equivalent to “Clear All” filters

My Campaigns

Clear out all filters and view all campaigns the user owns

My Active Campaigns

Clear out all filters and view campaigns the user owns but are not completed

Overdue Campaigns

Clear out all filters and view only campaigns that active and overdue

Creating a DSAR Campaign

To create a DSAR Campaign:

1. Open the DSAR Wizard by navigating to **Compliance > DSAR > DSAR Management > New DSAR**.

General Details

2. Provide an appropriate **Name** and **Description**.
3. Select the **DSAR Purpose** according to the type of campaign requested:

- Information Disclosure
- Data Redaction
- Data Deletion

4. Enter details and instructions for the reviewers to explain the request and what to check for in the validation stage. This text will be displayed in the review screen and the campaign email templates sent out for reviewers.
5. Enter a **Due Date** based on the due date type and date / length of campaign.
    - **After** - Set the length of the campaign. The due date will be set as this interval starting with the date the campaign is started.
    - **On** - Set the actual due date at time of creating the campaign.
6. Click **Next** to open the DSAR Query page.

DSAR Query

1. Select a **Scope Type** to target specific applications or application types. This will allow for the campaign results to be filtered by specific applications or application types.
    - All – Lists all applications defined in the system
    - Application Type – Select the appropriate application type(s)
    - Application – Select the appropriate application(s)
2. The query consists of one or more field matches. To add a field to the search, click the **+** button.
3. Add at least one search criteria. The more well-defined the search criteria is, the more accurate the results.

    The preset fields are:

    - Identifier
    - Address
    - Aliases
    - Email Addresses
    - Name
    - Phone #

> Multiple aliases and email address can be entered. Separate multiple values with a comma.

If marked **Required**, this value must be included in the file to satisfy the query. When selecting Required, the Relevancy Score will be calculated off that identifier.

4. Click **Next** to open the Review Process page.

Review Process

Set one or more reviewers to check this DSAR Campaign results. Reviewers can be individual users or groups of users.

There is an option on the next screen to configure sending invitations and reminders to the reviewers.

- Select the account type: User or Group
- Select an account by typing in part of the name, and selecting from the list.
- Click **Next** to open the Summary page

Summary

Review your DSAR campaign settings and configure notification and reminders for reviewers. Using the Save button options, you can choose to automatically run the campaign upon saving it, or save and manually run the campaign at a later stage.

Due Date

For campaigns with a fixed due date, or campaigns that had already started

DSAR Query

The query defining the identity to act on. The unique identifier values are partially obfuscated, displaying the last four digits / characters.

Scope

Provides the target applications associated with the campaign.

Request Purpose

Provides the reason for the campaign.

Review Process

Displays the number of reviewers. Click on the number to open a dropdown list of reviewer names.

Campaign Invitation

Select this option to have the system send an invitation to all the reviewers

Reminders Schedule

Select this option to send weekly email reminders to all reviewers with pending action, at 8 AM on Monday (local time)

1. Click **Save** to store the campaign without running.

   OR

2. Click **Save& Run** to start the campaign.

> If the campaign is only saved, the whole campaign will be editable. If the campaign is saved and ran, only the General Details and schedule will be editable.

DSAR Scope Management

Use this screen to define the scope of applications and application types for Data Subject Access Requests.

Only applications which support data classification and are governed by/through File Access Management will be available for Data Privacy scope setting.

By default, every application will include all resources in Data Privacy scans. By adjusting the scope, you can configure each application to include only a subset of resources in the Data Privacy related task.

To access the screen, navigate to **Compliance > DSAR > Scope**.

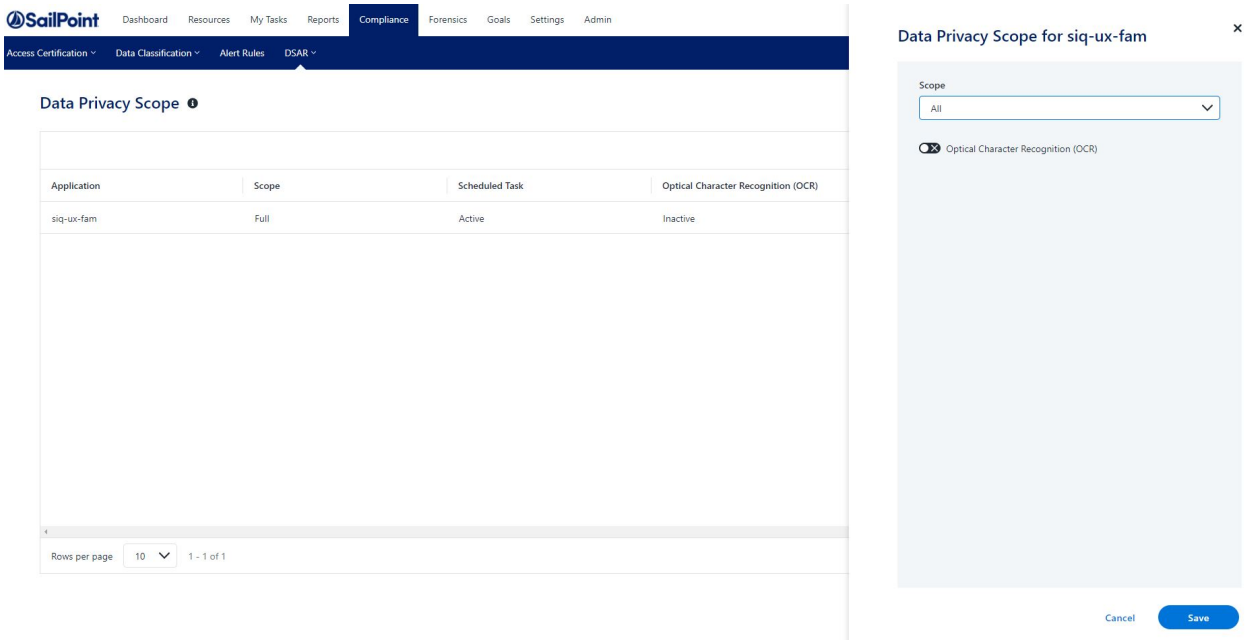
Editing the DSAR Scope

> Editing the scope is optional.

Navigate to **Compliance > DSAR > Scope** and complete the following steps to edit the DSAR scope:

1. Find the desired application from the DSAR Scope screen.
2. Click **Edit** to modify the scope (such as folders), and/or the OCR setting of the DSAR per application.

This will open the Data Privacy Scope Edit screen.



To change the scope to include in the DSAR process:

1. Select the scope type.
    - All – run DSAR on all the resources in the application
    - Resource – select an individual resource and whether or not to include all resources nested under it (all child resources)

2. Click **Optical Character Recognition (OCR)** to enable / disable OCR analysis for this application.

   If Resource was selected as the Scope type, a Resource field will display under Optical Character Recognition (OCR).

   > The OCR is defined by editing the application in **Admin>Applications>Edit**.

3. Select the desired resource.

   > Resources can be searched for using the search field.

   > Multiple resources can be selected.

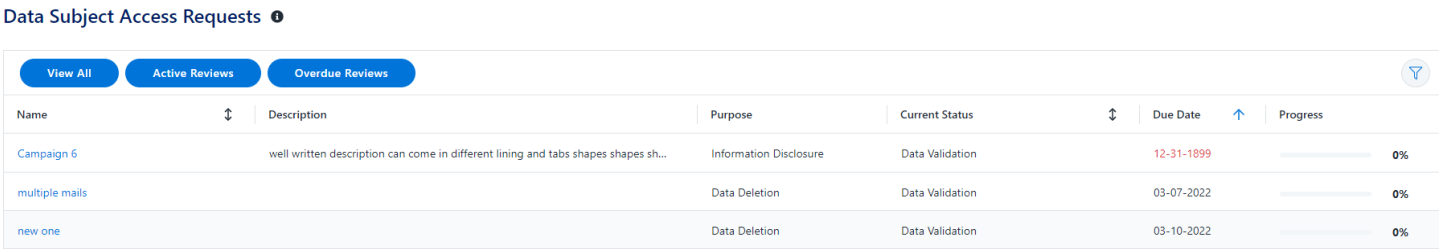
DSAR Requests Review

The DSAR review page displays all campaigns that are pending your review.

This screen includes tasks to validate and remediate data.

To review all DSAR campaigns, navigate to **My Tasks > DSAR**.

> The default filter setting is set to show Data Validation or Data Remediation in Progress.



Name

Name of the DSAR campaign

Description

Information about the purpose of the campaign

Purpose

Reason for the DSAR

Current Status

The campaign statuses can be one of the following:

- Created & Ready to Run
- Data Discovery
- Data Validation
- Remediation - In Progress
- Remediation - Completed
- Verification - In Progress
- Verification - Completed
- Completed
- Failed
- Pending Deletion

Due Date

The DSAR campaign deadline (date)

Progress

Indicates how many of the files within the campaign have been decided on.

The page provides the following three predefined options to filter between reviews:

- View All
- Active Reviews
- Overdue Reviews

Making Campaign Review Decisions

The predefined columns are:

File Name

Name of the file found in the data discovery phase

Full Path

Location where the file is stored

Relevancy Score

Calculated by the score of the items searched by the item count

Matched Terms

Displays what identifiers were matched from the query

Actions

Select the decision for the file. Available decisions are Confirm, Exclude, Comment

The user has different options on how to view information. These options display at the top of the Actions column:

- Export Results
- Filters
- Column Chooser

Export Results

Reviewers have the ability to export the results from the grid into a portable format (CSV), so that the results can be shared with other stakeholders that do not have access to File Access Management.

Filters

- Status – Choose statuses of the file
- Application Type – Choose applications the file is associated with
- Application – Choose created applications

- Resource Name – Name of the folder where the files are located
- Resource – Choose from a full scope
- Resource Full Path – Type the path where the file is located
- File Name – Enter the file name for the search
- File Type – Choose the file types of the file
- Relevancy Score – The user has three options to choose from. Select **Equals** and provide the exact value. Or choose **Higher Than** or **Lower Than** and provide a value.

Column Chooser

- Status – to display the current status of the record
- Application Type – to display the application the record is associated with
- Application Name – to display the application
- Resource Name – to display where the files are located
- File Type – to display the type of file the record is

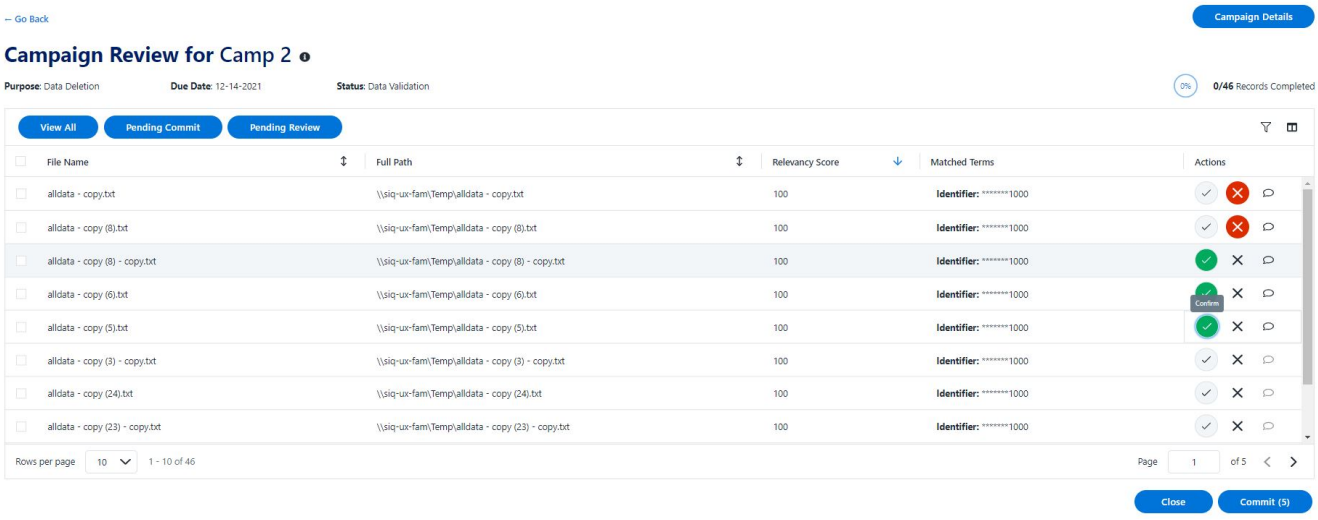
To make decisions on the selected campaigns:

1. Select the desired campaign to view that particular campaign review page. To select a campaign, click the blue campaign name.

   Depending on what data was discovered, a variety of files will display.

   If the user is wanting to find specific campaigns, there are filtering options at the top left of the grid.

   - View All – view all files that were discovered
   - Pending Commit – view only files that are waiting to be committed
   - Pending Review – view only files that need to be reviewed



2. To the left of each file is a box. Click on the box of the desired campaign to provide your decision.
3. Once a file is selected, a decision can be made one of two ways. Either:
    a. Select one of the newly displayed options at the top of the grid. The options are:
    - Clear – remove any decisions which have been made but not committed
    - Confirm – accepts the record
    - Exclude – remove selected record from the decision process

    > If Exclude is selected for any record, providing a comment is optional

    b. Select an action from the Actions column.

    > The actions are the same as above.

4. Click **Commit** once all desired files have been reviewed and have a decision.

    The review will end when all result decisions are made and committed.

> Clicking **Close** takes the user back to the main campaign review page.

DSAR Campaign Details

Once the campaign decision(s) have been made, the campaign creator will be able to review the decision(s) made by navigating to **Compliance>DSAR Management** and clicking the desired campaign.

On the Campaign Details screen, the user will see the name of the Campaign and the following below the Campaign name:

- Purpose – type of DSAR that was requested
- Due Date – campaign deadline
- Status – provides the status of the campaign in its current phase.

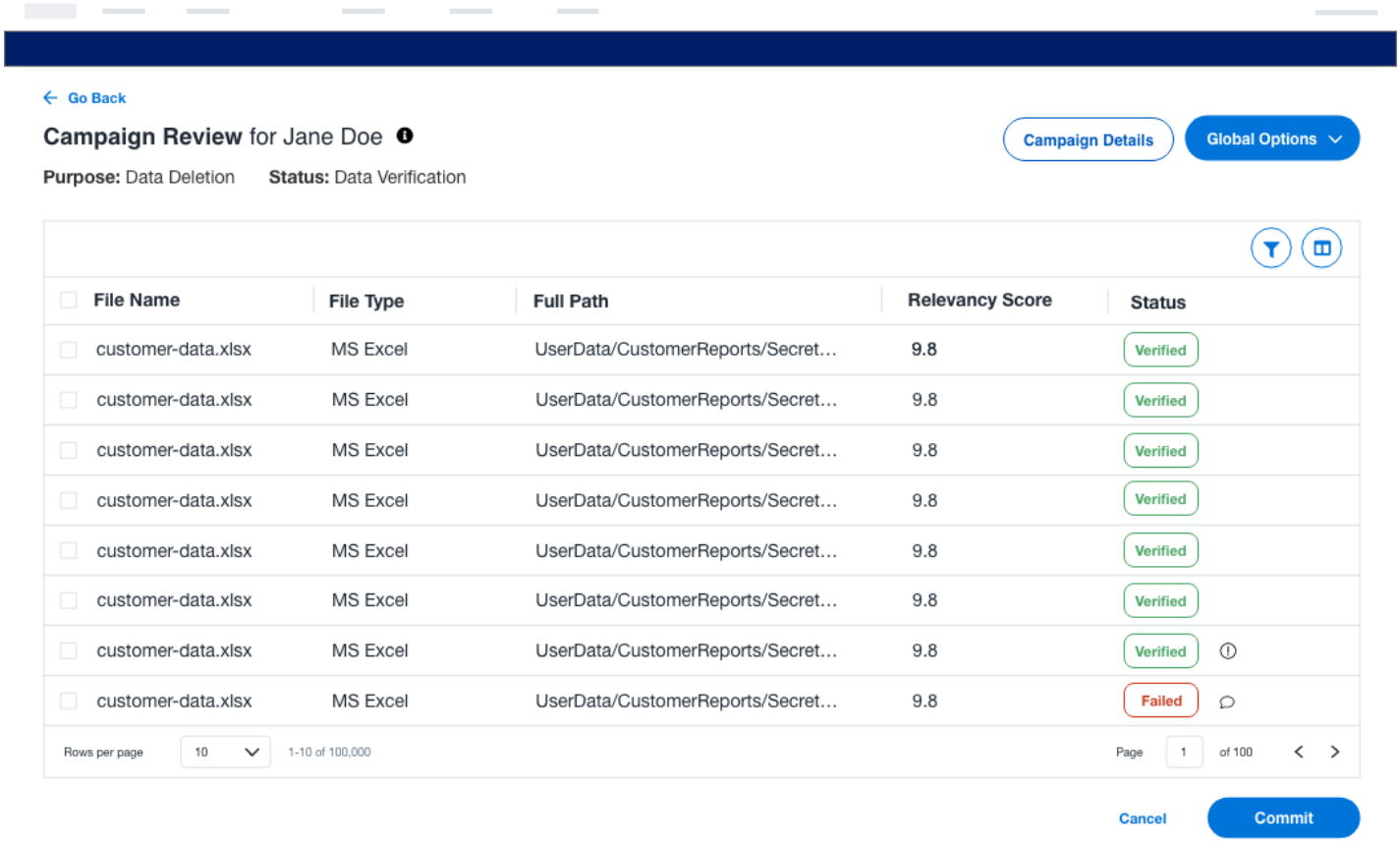
All files that were discovered will be listed as well as their full file path.

Also displayed is the relevancy score. This is calculated based on required and non-required fields. The Identifier field is required while the Name field is not.

> If both are found, the result will equal 100.
> If only the Identifier is found, the result will equal 50.

The last column will show the status of the files in the campaign.

Administrator Review



If a campaign is in the data verification stage, the user will be able to click on a non-verified or failed report. If the report failed, you can see the reason for the failed verification.

The user will then have the option to do one of the following for both non-verified and failed reports:

- Exclude – ignore the failed verification and provide a (optional) comment
- Override – override the failed verification and provide a (optional) comment

If the failed verification was ignored, the status will change to Verified with Exceptions

If the failed verification was overridden, the state will change to Verified.

If the verification was successful, the record will show as Verified.

Exclude / Override

If multiple records are selected, the user can click the Exclude/Override Verification button that displays at the top right of the screen.

This gives the user the ability to deal with records in bulk, rather than handling each individual record.

Reassigning Reviewers

Compliance administrators will be able to reassign items that are pending review from one reviewer to another.

1. Once the desired file(s) is selected, click **Reassign Reviewers** which will open a new display.
2. Select the current reviewer from the Current Reviewer dropdown.
3. Select the new reviewer from the New Reviewer dropdown.

   Comments are not required, but are made available if a user desires to leave a comment.
4. Click **Reassign**.

DSAR Reports

Running a DSAR campaign allows the user to also generate a report.

From the DSAR Management screen, click the Generate Report icon under the Actions column to create a report of any desired campaign.

A message will appear notifying that a report is being generated and will be available in My Reports.

When the report is complete, a bell notification will be displayed notifying the report can be viewed or downloaded.

Once the report is opened, six tabs with various information will be available. This allows the user to get a snapshot of the campaign within its different phases.

Report Summary

This tab lists report generation details, DSAR campaign query and scope, campaign details, aggregations

Data Validation

This tab lists all records and review decisions in the data validation phase

Data Remediation

This tab lists all records and review decisions in the data remediation phase

Data Verification

This tab lists all records and reviews decisions in the verification phase

Excluded Records

This tab lists all excluded records, the review decisions and exclusions comments

Information Discovered

This tab presents all of the personal information discovered during the process

DSAR Bulk Operations

Running a bulk operation allows administrators to submit a list of records to be searched, such as a list of names, emails, and address combinations. These large requests will reach the responsible party in bulk, and will need to be handled in bulk to avoid unnecessary additional work.

See Bulk Campaign Creation to understand how to create and run bulk campaign.

A user also has the ability to perform bulk actions on campaigns. To see each bulk action available, see Bulk Actions.

Bulk Campaign Creation

To create a bulk campaign, navigate to **Compliance>DSAR>DSAR Management>Bulk Create**.

To run a bulk campaign, a data source has to be identified. From the drop down, select the appropriate data source for the campaign.

File Access Manager allows the user to import campaigns in bulk using a data source.

> If a data source needs to be created or edited, navigate to **Admin>Data Source**. For more information on data sources, see Data Source Types and Usages.

1. Select a campaign field to be mapped.

   The identifier field mappings are:

- Campaign Name
- DSAR Purpose
- Due Date
- Identifier
- Name
- Aliases
- Address
- Email Addresses
- Phone

> Multiple aliases and email address can be entered. Separate multiple values with a comma.

2. Map at least one Review field. This can either be Review Users or Review Groups.

A pop up will display allowing the user to verify the bulk creation.

3. Click **Create** to store the campaign without running.

   OR

4. Click **Create & Run** to start the campaign.
5. Click **Yes** or **Cancel**.

If Yes was clicked, a message will display stating that a task to run the campaign(s) was created and the progress of the campaign can be monitored at **Task Management>Tasks**. An automatic email will also be sent to the reviewer so that they are notified of a new campaign they need to review.

Bulk Actions

Running Campaigns in Bulk

If a user wants to initiate the data discovery and review process tasks, navigate to **Compliance>DSAR>DSAR Management**.

1. Select the desired amount of campaigns.
2. Click **Run Campaigns**.

   A confirmation will display. The pop up will ask the user to confirm the running of the number of selected campaigns.
3. The user can click either **Yes** or **Cancel**.

Verifying Campaigns in Bulk

To verify that the personal data identified through the campaign(s) have been remediated, navigate to **Compliance>DSAR>DSAR Management**.

1. Select the desired campaigns.
2. Click **Verify Campaigns**.

   > This task will only start with campaign statuses of Remediation - Completed.

   A confirmation will display. The pop up will ask the user to confirm the verification of task of selected campaigns.
3. Click either **Yes** or **Cancel**.

Canceling Campaigns in Bulk

To cancel the campaign(s) execution, review process or avoid any further changes to the campaign(s), navigate to **Compliance>DSAR>DSAR Management**.

1. Select the campaigns.
2. Click **Cancel Campaigns**.

   > This task will only start with campaign statuses of Data Discovery.

   A confirmation will display. The pop up will ask the user to confirm the canceling of the number of selected campaigns.
3. Click either **Yes** or **Cancel**.

Ending Campaigns in Bulk

To finalize the campaign(s) review process, end the execution process and prevent any further changes, navigate to **Compliance>DSAR>DSAR Management**.

1. Select the campaigns.
2. Click **End Campaigns**.

   A confirmation will display. The pop up will ask the user to confirm the ending of the number of selected campaigns.
3. Click either **Yes** or **Cancel**.

Deleting Campaigns in Bulk

To permanently remove all information related to the campaign(s), including the DSAR query results, progress history, pending and committed conclusions, and associated comments, navigate to **Compliance>DSAR>DSAR Management**.

1. Select the campaigns.
2. Click **Delete Campaigns**.

   A confirmation will display. The pop up will ask the user to confirm the deleting of the number of selected campaigns.
3. Click either **Yes** or **Cancel**.

Remediating Campaigns in Bulk

To queue a task to scan all data assets involved in the selected campaign(s) and to verify that the personal information identified through the campaign(s) have been remediated, navigate to **Compliance>DSAR>DSAR Management**.

1. Select the campaigns.
2. Click **Remediate Campaigns**.

   A confirmation will display. The pop up will ask the user to confirm the remediation of the number of selected campaigns.
3. Click either **Yes** or **Cancel**.