



PUBLIC

SAP Fieldglass

SAP Fieldglass - Managing Job Seeker, Worker, and User Privacy

Content

- 1 Privacy. 3**
 - 1.1 Erasing a User. 4
 - 1.2 Reporting on Personally Identifiable Information. 4
 - 1.3 Managing Data Retention Policies. 5
 - Managing Data Retention Policy Setup. 7
 - Managing Data Retention Policies Usage. 11
 - SAP Fieldglass - Erasing Your Personal Information. 22
 - SAP Fieldglass - Erasing a Worker/Erasing a Supplier User. 23
 - SAP Fieldglass - Erasing a Worker/Erasing a Buyer User. 24

1 Privacy

Protecting the rights and freedoms of data subjects is very important to SAP Fieldglass. Functionality is available that can be used to erase a person's records from the application.

Caution

Per your contract with SAP Fieldglass, sensitive data should not be entered in native or custom fields. Sensitive data includes, but is not limited to, the following: non-public government identification numbers, individual financial account numbers (Social Security numbers, insurance numbers, driver's license numbers, credit card numbers, or banking numbers), medical records, health care claims, information associated with the International Traffic in Arms Regulations, data that is restricted by law, or sensitive technical data. Refer to Section 2 of your contract for more details.

Data Subjects

Data subjects are people that use the SAP Fieldglass application. They can be users, job seekers, workers, or resources.

Users

These are people who work for a buyer or supplier organization and use the SAP Fieldglass cloud service. When these individuals leave the organization, it may be necessary to erase their records. Buyers and suppliers have a simple action to erase user records that is not tied to any configuration. The user must be in *Closed* status to use this functionality. Refer to [Erasing a User \[page 4\]](#) for more information.

Job Seekers, Workers, and Resources

When suppliers create a draft of a job seeker record, but no action is taken on it for more than seven days, the application automatically deletes the record. This deletion occurs regardless of whether or not Managing Data Retention Policies is enabled.

Functionality is available for buyers called Managing Data Retention Policies. When enabled, it can be used to erase personally identifiable information (PII) from documents in the SAP Fieldglass cloud service related to Job Seekers, Workers, and Resources, including Attachments. Refer to [Managing Data Retention Policies \[page 5\]](#) for more information.

1.1 Erasing a User

Buyers and suppliers have an action available to erase user records which provides them a simple way to manage the data of individuals who no longer use the SAP Fieldglass cloud service and need to be removed.

Enable User Role Permission

There is no company configuration needed to use this functionality. Buyer and supplier users must be administrators or in a role with the user role Administrative Permission ► [User](#) ► [Erase Closed Users](#) ► enabled.

Erase User Data

When a user with permission accesses the User record of a closed user, the [Erase](#) button displays. When the button is selected, a warning message displays. If confirmed, the user is placed in [Pending Erasure](#) status for 14 days and the option [Undo Erase](#) is available. After 24 hours, the user is erased in the SAP Fieldglass application.

Erased Data

When a user is erased, the data is erased in the following manner:

- The name and email information is replaced with 'XXXX'. Cc emailaddresses are erased.
- The Profile Picture is deleted.
- The Employee ID and Contact Information is erased.
- User Profile fields such as Supervisors and Signature Authority are erased. Feature Access fields are disabled.
- The user is no longer available for selection from any modals or list views.
- If the user appeared in any document, work item, or system audit trail, their name is replaced with 'XXXX'.
- The user no longer displays in any reports.

Integrations

The upload, [Standard User Data Erasure Upload](#) can be used by buyers and suppliers to erase closed users. The upload only requires the usernames of the closed users.

1.2 Reporting on Personally Identifiable Information

Buyers and suppliers can run reports on Personally Identifiable Information data.

To locate Personally Identifiable Information reports, navigate to ► [Analytics](#) ► [All Reports](#). ► Select [Personally Identifiable Information](#) from the [Base Module](#) dropdown menu and choose a report.

To run the report, select [Run](#) from the report run screen. For more information on reports, refer to the SAP Fieldglass Analytics guide.

Report:	Description:	Visibility Settings:
PII Audit	Provides a history of changes to Personally Identifiable Information fields.	Buyer and supplier administrators have access to this report by default. Other user visibility to reports is determined by assigning user roles to report folders. The View Personally Identifiable Information report user role permission must be enabled to view this report.
Contingent Job Seeker or Worker Personally Identifiable Information	Displays the Personally Identifiable Information (PII) for an individual based on the first and last name entered. This predefined report includes Personally Identifiable Information fields. You can create a custom report by copying and editing this report to manually add other native and custom fields that might contain PII.	Buyer administrators have access to this report by default. Other user visibility to reports is determined by assigning user roles to report folders.
SOW Worker or Resource Personally Identifiable Information	Displays the Personally Identifiable Information (PII) for an individual based on the first and last name entered. This predefined report includes Personally Identifiable Information fields. You can create a custom report by copying and editing this report to manually add other native and custom fields that might contain PII.	Buyer administrators have access to this report by default. Other user visibility to reports is determined by assigning user roles to report folders.

Log of User Activity

Buyers can request a report that identifies specific pages users have viewed and any attachments they have opened. SAP Fieldglass database administrators will run a query directly against the database for this report and deliver the results to the buyer. To request this report, contact your SAP Fieldglass representative.

1.3 Managing Data Retention Policies

The Managing Data Retention Policies functionality allows buyers to set thresholds for automatically identifying job seeker, worker, and resource records that may need to be erased.

A buyer organization may have data retention policies that mandate that any information which can be used to personally identify an individual should be erased after a defined period of time. The definition and related

terminology for personal information can vary from country to country, but for this content the term Personally Identifiable Information (PII) is used.

It is very common for these data retention policies to extend to the buyer's external workforce requiring a buyer to manage the relevant information that is stored on an SAP Fieldglass record. For example, a data retention policy could state that five years after a worker ends an assignment, the worker's name, email address, and resume/CV should be erased from all related SAP Fieldglass records. Additionally, workers, resources, and job seekers sometimes request that their PII be erased from the application prior to when the thresholds established by the buyer have been met.

When a buyer is assessing its PII needs, there are two common scenarios:

- A person applied, but was not selected for an assignment or did not start it. (Job Seekers)
- A person did work for the buyer organization. (Workers and Resources)

To ensure buyers can manage their PII data retention policies, the Managing Data Retention Policies feature offers the following:

- The Personally Identifiable Information admin object (this is the area of the application where buyers can view and take action on all records that are eligible for erasure).
- Buyer-defined thresholds that automatically identify which records are eligible for erasure.
- Leveraging the buyer-defined thresholds, eligible records are displayed in several list views where buyers can take action. List views include Job Seekers, Workers (including Resources), and Attachments.
- For the selected records, PII data is permanently erased and an audit history is maintained.
- Buyer users can search for a worker, resource or job seeker record which has not met the predefined thresholds and select them for erasure on an ad hoc basis.
- Large volumes of job seekers, workers, resources, and related attachments can be managed via integrations.

This functionality erases certain personal information but does not erase all data from the SAP Fieldglass cloud service. This is because some data is controlled by other organizations and individuals. For example, the worker controls the data on the worker profile and a supplier controls the data on a workforce record.

When an organization or individual requests data erasure of personal information, SAP Fieldglass can help facilitate the request from a data processor perspective; however, the organizations and individuals need to use the administrative functionality/tools within the SAP Fieldglass cloud service to actively remove any relevant personal data. The following documents can be given to appropriate organizations or individuals to provide more technical details on the steps they need to take within the cloud service to erase the relevant personal data the organization or individual controls:

- [SAP Fieldglass - Erasing Your Personal Information \[page 22\]](#) – This document can be given to workers who want to erase themselves in the cloud service.
- [SAP Fieldglass - Erasing a Worker/Erasing a Supplier User \[page 23\]](#) – This document can be given to suppliers who want to erase a worker or supplier user.
- [SAP Fieldglass - Erasing a Worker/Erasing a Buyer User \[page 24\]](#) - This document can be given to buyers who want to erase a worker or buyer user.

Related Information

[Managing Data Retention Policy Setup \[page 7\]](#)

1.3.1 Managing Data Retention Policy Setup

To use this functionality, some setup is required.

Company Configuration

In order to use this functionality, the company configuration [Data retention policies](#) must be enabled.

User Profile Flag

When the configuration is enabled, the user profile flag, [Manage Personally Identifiable Information](#), is available. It must be enabled for individual users to see the **Personally Identifiable Information** list view. This flag cannot be enabled if the MSP User flag is set to [Yes](#). Users without the flag enabled are not able to view the list view or select records to be erased.

Note

Once you've enabled the Data retention policies company configuration and the Manage Personally Identifiable Information user profile flag, the [Personally Identifiable Information](#) admin object is available in the Admin menu. This is where records that are eligible for erasure display and can be acted on.

Custom Lookup - Personally Identifiable Information Thresholds

Once the company configuration is enabled, if you want to automatically identify records that should be considered for erasure, you must set up thresholds for Personally Identifiable Information (PII). Time thresholds that determine which records are eligible for data erasure can be defined for:

- **Job Seekers** (people who are in any status other than Hired or Draft) - This threshold is the number of days since the job posting close date. Work order (Contingent and SOW) and SOW worker records that aren't fulfilled and are in Rejected, Closed, or Withdrawn status are included with job seekers based on the number of days since the SOW work order was moved to the status.
- **Workers** (people who have been hired) - This is the number of days since the actual end date of the worker (both contingent and SOW workers).
- **Statement of Work Attachments** (attachments on SOW invoices and credit/debit memos) - This is the number of days since the statement of work was closed. This threshold does not apply to SOW workers. The worker threshold applies to SOW workers.
- **Resources** (people who have been hired as a Resource type of worker on a statement of work) - This is the number of days since the resource was closed.

- **Historical Workers** (people who have been hired in the past and whose records have been uploaded using a connector) - This is the number of days since the end date of the historical worker.

Erasure for decision forms are affected by the thresholds mentioned above. When a decision form is completed with a Job Posting with Named Resource, Profile Worker, Project, or Statement of Work with Named Resource procurement type and is tied to another record (a job posting, statement of work, et cetera), all PII fields and all attachments on the decision form are moved to the Job Seeker threshold when the last associated record gets erased.

Note

If the company configuration is enabled but the thresholds are not created, you can still use the functionality to search for records and erase them.

Refer to [Custom Lookup - Personally Identifiable Information Thresholds \[page 9\]](#) for more information on this custom lookup.

If Tenure functionality is being used by your company, remember to consider the duration of your Tenure thresholds when creating your Personally Identifiable Information threshold. For more information about Tenure, refer to the SAP Fieldglass Tenure Policy Management guide.

User Role Permission

The PII Audit report, which reports on changes to Personally Identifiable Information fields, is available to buyers administrators and suppliers by default. The [View Personally Identifiable Information report](#) user role permission is required in order for users to view this report.

Custom Fields

When the configuration is enabled, custom fields for some modules include the field, [Personally Identifiable Information](#). When creating or editing custom fields, Yes can be selected in this field to indicate if the custom field content will contain PII. If enabled for a custom field, the field is erased when a record is selected for erasure. Also, the custom field admin object list view includes a column for this field. The column displays N/A when the custom field is for a module that does not have the Personally Identifiable Information flag.

If this new flag has been selected and the custom field is linked to the Job Posting, Job Seeker, Work Order, Worker, or SOW Worker modules, the linked custom field automatically has the PII flag enabled.

Activity Item

When the configuration is enabled, activity items where attachments are captured include the field, [Personally Identifiable Information](#). When creating or editing an activity item, Yes can be selected in this field to indicate if the attachment will contain PII. If enabled for an activity item, the attachment is erased when a record is selected for erasure. If the activity item is not flagged as having attachments with PII, the attachment is

included in the Attachment list view where it can be manually reviewed to determine if PII exists and erased if necessary.

Custom Lookup - Personally Identifiable Information Thresholds

Used to create thresholds to automatically identify job seeker, worker, resource, and statement of work attachment records that should be considered for erasure.

Only one Custom Lookup with this Lookup Type can be created. When it is selected, there are three segments automatically created. These are the only segments allowed.

- **Module** - On the upload file, this is the first segment. It should contain Job Seeker, Worker, Resource, Historical Worker, or Statement of Work (SOW Invoice and SOW Credit/Debit Memos). These are the four modules for which a threshold can be established. Only one module can be included in a row on the upload file.
- **Site Code** - On the upload file, this is the second segment. It should contain a valid site code. This allows the buyer to establish thresholds at the site level. If all sites should have the same threshold for the module, enter [ALL] (including the brackets) instead of the site code. Multiple sites cannot be included in one row on the upload file. For the Resource module, the Site Code must be [ALL].
- **Threshold** - On the upload file, this is the third segment. It should contain the number of days for the threshold. For Job Seekers, this is the number of days since the job posting close date or the number of days since the SOW work order was moved to the status, Rejected, Closed, or Withdrawn. For Workers, this is the number of days since the actual end date of the worker including SOW worker. For Resource, this is the number of days since the resource was closed. For Statement of Work, this is the number of days since the statement of work was closed and it only applies to SOW invoices and Credit/Debit Memos.

→ Remember

When configuring your Personally Identifiable Information threshold, it is important to consider whether Tenure policies are being used by your company and the potential impact of conflicting threshold durations. A Personally Identifiable Information threshold with a duration that does not last long enough to accommodate for Tenure policies could result in the erasure of records that are still needed for Tenure. Always consider the duration of your Personally Identifiable Information custom lookup threshold in relation to your Tenure custom lookup threshold and configure them accordingly.

Use the information in this table to create the custom lookup.

Field	Description
Name	Enter a name for this custom lookup. This differentiates the lookup from other lookups and displays in drop-down lists when a custom lookup needs to be selected. The name must be unique, it can't include commas, and can be up to 100 characters.
Lookup Type	Choose the type of custom lookup you want to create. The options available depend on how your company is configured. Select Personally Identifiable Information Thresholds .

Field	Description
Data Set	This optional field only displays when the company configuration, Data set, is enabled. The data set must be created before it can be selected from this dropdown. When a data set is selected, the data combinations for the lookup come from the data set. For more information about data sets, refer to the topic.
Number of Segments	The number of attributes required for the lookup. This number corresponds to the number of headers that can be defined. If a data set is associated, this number defaults and can't be changed.
Delimiter	The character used in the upload file to separate the values in each column. Available delimiters: • ; (semicolon) • (pipe) • - (dash) • : (colon)
#	The number of the segment and the order in which it displays on the custom lookup. The first segment is the first column on the custom lookup. Values must be uploaded in this order.
Header Type	Select either Key or Value. • Keys are the data elements that drive the lookup. These data elements correspond to information on a document or record in SAP Fieldglass, or to the associated documents or records. This data can be system generated or ad-hoc user-entered data. • Values are the retrievable results or outputs of the lookup. The values are typically derived from the relationship of the keys. These outputs are always provided by the lookup when it's being used. The Keys must be the first segments and the Values are the last segments.
Lookup Header	Select the data element for each Key and Value segment of the lookup. The options available depend on the Lookup Type and your company's setup.
Key	Available Key options include: • Module • Site Code
Value	The only available Value option is Threshold.

1.3.2 Managing Data Retention Policies Usage

Describes how to use the Manage Personally Identifiable Information list views and Personally Identifiable Information admin object to erase data.

Personally Identifiable Information Admin Object

Once the functionality has been set up, users see the *Personally Identifiable Information* admin object under the *Past Data* section of the Admin menu.

The admin object contains the View menu and three tabs at the top where records display in list views. The tabs include:

- *Records Past Threshold* - Records that are past their threshold.
- *Queued Records For Erasure* - Records that have been selected for erasure and are set to be erased 14 days from the time they were selected.
- *Search Records* - Users can search for worker, resource, or job seeker records using the record ID and erase them. This action moves the record into the Queued Records for Erasure list.

View Menu

The View menu options include:

- *Job Seekers* - This view includes records of job seekers who didn't become workers, who are in a status other than Hired or Draft, work order (Contingent and SOW), Decision Forms, and SOW worker records that weren't fulfilled and are in Rejected, Closed, or Withdrawn status. A job seeker displays on this list when the threshold has been met based on the job posting close date (the job posting must first be closed in order for a Job Seeker to be displayed). A contingent work order displays when the threshold has been met based on the number of days since the contingent work order was moved to withdrawn status. An SOW work order displays when the threshold has been met based on the number of days since the SOW work order was moved to the status Rejected, Closed, or Withdrawn. For example, a job seeker is submitted on a job posting, the person is never hired or confirmed, therefore, there is no worker record. The buyer's threshold for job seekers is 90 days. Ninety days after the job posting is closed, the job seeker displays on this list view. Decision forms, once erased, are displayed in the Job Seeker threshold. When a decision form is completed with a named resource and is tied to another record (a job posting, statement of work, et cetera), all PII fields and all attachments on the decision form are moved to the Job Seeker threshold when the last associated record gets erased.
Note that when suppliers have drafted a job seeker record, but no action has been taken on it for more than seven days, the application automatically deletes the record whether or not the Managing Data Retention Policies functionality is enabled.
- *Workers* - This view includes workers, historical workers, and resources in Closed status when the threshold has been met based on the actual end date of the worker or resource. For example, a job seeker is hired and confirmed and a worker record is created. The buyer's threshold for workers is 1095 days. When the actual end date of the worker is passed 1095 days, the worker displays on this list view.
- *Attachments* - This view includes attachments related to records displayed in the job seekers and workers list views including attachments added to the documents created from the job seekers and workers. Additionally, when any of the following documents have an attachment, the attachments display on this list view when the worker from which the document originated has met the company's established worker threshold (Expense Sheet, Invoice, Consolidated Invoice, SOW Invoice, Miscellaneous Invoice,

Credit/Debit Memo, or SOW Credit/Debit Memo). If there is an activity item on the worker with the Personally Identifiable Information flag set to Yes, the attachment on the activity item is erased when the worker is selected to have personal information erased. If the flag is set to No, the attachment is included on this list. **Note:** Some attachments will not show in this list view as they will automatically erase along with the erasure of the Job Seeker or Worker record. This includes resume, activity items with the Personally Identifiable Information flag set to Yes, and Qualifications with Assessment Scale of Certification and Require Attachment set to Yes.

Note

If the buyer company has the company configuration *Preservation indicator to prevent archiving or data erasure* enabled and the *Turn Preservation On* flag is enabled for a job seeker, statement of work, resource, or any other worker type record, it does not display on the list views and cannot be erased until the flag is turned off.

Erasing Data

From the list view, the user can select the items that should be erased. To erase the data:

- The user selects the checkbox preceding the item and then selects the *Erase* button. A warning message displays.
- When the user selects *Confirm* on the warning message, the items selected are added to the *Queued Records For Erasure* list.
- Items in the *Queued Records For Erasure* list stay in the list for 14 days before the personal information is permanently erased. During that time, the action can be undone by going to the *Queued Records For Erasure* list, which is a link to the right of the *Records Past Threshold* list, selecting the checkbox preceding the item and then selecting the *Undo* button. If the action is undone on a record that doesn't meet the thresholds (see Search Records below), the record no longer displays in the Personally Identifiable Information list views.

Once items are actually erased, the action is permanent. The numerical part of the document ID is changed to X's when the record is erased. An audit history of this action is logged. Once a worker or resource record is erased, the options to Reopen, Edit Worker, Reset Password, or Change Profile Picture no longer display. If the company configuration *Preservation indicator to prevent archiving or data erasure* is enabled, the Turn Preservation On option is also removed.

Actions, social messages, and the starred button are unavailable for records in the erasure queue and all records related to erasure queue records to prevent a buyer or supplier from accidentally reopening a record. If just an attachment on a record is erased, actions remain available for that record.

Supplier Notification/Action

When records are added to the *Queued Records For Erasure* list by the buyer, relevant suppliers are notified and have 14 days to review these records before permanent erasure. Additionally, suppliers must manually erase all workforce records connected to these records in the Queued Records For Erasure list to ensure that all personally identifiable information is fully erased. Suppliers are also notified when records are removed from the Queued Records For Erasure list.

Suppliers are able to add the reporting field, *Pending Erasure?* on Job Seeker, Worker, Worker Order, and Resource module reports, allowing them to view and create reports on records in the erasure queue. The supplier user role permission, *View Records Pending Erasure*, is required in order to add this reporting field.

Search Records

Workers, resources, and job seekers sometimes want their PII to be erased from the application prior to when the thresholds established by a buyer have been met. The [Search Records](#) tab on the Personally Identifiable Information list view allows the user to search for workers, resources, and job seekers using the full ID, for example, XXWK00012345. Buyers can use this search feature even if they have not established any thresholds as long as the configuration is enabled and the user has the profile flag enabled. The search only retrieves records based on the following criteria:

- Job seekers cannot be in **Confirmed** status and the associated job posting must be in Closed status.
- Workers and resources must be in **Closed** status.
- Job seekers and workers cannot have the **Turn Preservation On** flag enabled.

The user can choose which of the worker, resource, or job seeker records to erase including attachments. Once selected to be erased, the records are moved to the [Queued Records For Erasure](#) tab.

Download Data

When a user is viewing the [Records Past Threshold](#) for Job Seekers, Workers, Resources, or Attachments, the list view displays a maximum of 100 records. The link **Save as CSV** does not pull all the records if there is a large number. To accommodate large numbers of records, there is a button on the tab, [Download All Data](#). This button allows the user to download all the records for the specific view into a CSV file format. The ID and Name columns can be copied into one of the uploads (see below) to erase a large number of records.

Integrations

Two uploads are available that allow buyers to erase large volumes of data:

- [Standard Job Seekers and Workers Data Erasure Upload](#) - This upload is used to erase job seekers, workers, and resources. In addition to the ID and Name columns, there are two additional columns. The Adhoc column should be set to No if the record meets the data erasure thresholds or Yes if it does not meet the thresholds. The Erase Attachments column is used to indicate that the attachments (other than the ones automatically erased when the job seeker or worker is erased) should also be erased. Set it to No if the attachments should not be erased or Yes if they should. When Yes is used, there is no need to use the Standard Attachment Data Erasure Upload to erase the attachments separately.
- [Standard Attachments Data Erasure Upload](#) - This upload is used to erase attachments that are not automatically erased when the job seeker, resource, or worker is erased. In addition to the ID and Name columns, there is an additional column. The Adhoc column should be set to No if the record meets the data erasure thresholds or Yes if it does not meet the thresholds.

When records are erased via an upload, the records display on the Queued Records for Erasure tab for 14 days prior to being permanently erased. The action can be undone via the UI during that 14-day period.

Related Information

[Erased Data \[page 14\]](#)

Erased Data

When the Personally Identifiable Information list views are used to erase data, the worker, resource, or job seeker's information is scrubbed in the SAP Fieldglass application.

When PII data erasure occurs, the Job Seeker, Resource, or Worker record itself remains in SAP Fieldglass, but all related PII is removed. The erasure action ensures that values in PII fields are replaced with characters such as "XXXX" or blank values, relationships to other records are removed as appropriate, and attachments known to contain PII are deleted.

The specific PII data that is erased is determined by the list view from which the record was selected. Detailed information for each list view is provided in this document. At a high level, the following PII data erasure actions occur:

- Select native fields are erased.
- Custom fields and linked custom fields with the PII flag enabled are erased.
- Resume/CV is deleted.
- The History tab on Workforce records is updated to remove references to related documents.
- The Consolidated Worker is updated to remove references to related documents and selected fields are erased.
- Activity Items with the PII flag enabled are deleted.
- An audit entry with the time stamp and user initiating the erasure is logged.

Reference ID

When a record is erased using the Personally Identifiable Information list view, the 14 character reference ID is replaced with a new number. This allows the record to be anonymous while still supporting uniqueness for purposes of report output. The format of the replacement number is: the first three or four positions remain the buyer or supplier code, the next two positions are replaced with X and another letter A-J which identifies the module (see list), the final eight positions are numbers. The eight numbers are generated consecutively for the module. An example of a replaced number for the job posting module is INFOXA00000001, INFOXA00000002, etc.

Module List

- Job Posting - XA
- Job Seeker - XB
- Work Order/Work Order Revision - XC
- Work Order Change Request - XD
- Worker - XE
- SOW Worker - XF
- Profile Worker - XG
- Consolidated Worker - XH

- Time Sheet - XI
- Expense Sheet - XJ
- Decision Forms - XK
- Historical Worker - XL
- Resource - XK
- Resource Time Sheet - XO

Note

Erasing a resource also erases all the PII contained within the Resource Time Sheet of that resource.

Related Information

[Job Seeker List View \[page 15\]](#)

[Worker List View \[page 17\]](#)

[Attachment List View \[page 18\]](#)

[Personally Identifiable Information Data Fields \[page 19\]](#)

Job Seeker List View

When the Personally Identifiable Information (PII), Job Seeker list view is used to erase data, the job seeker's information is scrubbed in the SAP Fieldglass application.

In situations where suppliers have drafted a job seeker record, but no action has been taken on it for more than seven days, the application automatically deletes the record whether or not the Managing Data Retention Policies functionality is enabled.

Job Seeker List View

The following table provides SAP Fieldglass's default best practice for job seeker data fields that are erased on records selected from the Job Seeker list view.

PII Data Erasure Action	Description
PII native fields erased	Modules: Job Posting, Job Seeker, Work Order, Interview, Social Enterprise Note: For Job Posting PII fields, data is erased when the last submitted Job Seeker is selected if no Worker exists. Otherwise, the PII on the Job Posting will be erased upon selection of the final Worker.

PII Data Erasure Action	Description
PII custom fields erased	Modules: Job Seeker, Work Order, Decision Form
Resume/CV deleted	The Resume/CV is removed from the Job Seeker record.
Workforce records updated	The History tab is updated to remove Job Seeker, Work Order, and Job Posting.
Activity Items with PII attachments deleted	Attachments with the PII flag enabled are removed from applicable Activity Items. Note: Attachments on the Job Seeker, Work Order, Interview, Social Enterprise or Activities (that do not have the PII flag enabled) will be displayed in the Attachment List View for review and potential deletion.

Job Seeker List View Statuses

The Job Seeker list view is intended to show all individuals who were submitted against any Job Postings for review, but who were not selected for the open position(s). The following statuses will be considered and displayed, based on a buyer-defined value of [x] days after the Job Posting Close Date.

- Work Order Accepted
- Work Order Activated
- Work Order Approval Paused
- Work Order Created
- Work Order Declined
- Work Order Draft
- Work Order No Show
- Work Order Pending Approval
- Work Order Pending Review
- Work Order Rejected
- Work Order Closed
- Work Order Deleted
- Work Order Pending Submission
- Work Order Withdrawn
- Job Seeker Closed
- Job Seeker Deleted
- Job Seeker Interviewed
- Job Seeker Rejected
- Job Seeker Shortlisted
- Job Seeker Submitted
- Job Seeker Withdrawn
- Job Seeker Draft
- Decision Form Rejected
- Decision Form Closed
- Decision Form Withdrawn

Worker List View

When the Personally Identifiable Information (PII), Worker list view is used to erase data, the worker's information is scrubbed in the SAP Fieldglass application.

Worker List View

The following tables provide SAP Fieldglass's default best practice for PII data fields that will be erased on records selected from the Worker list view.

PII Data Erasure Action	Description
PII native fields erased	Modules: Job Posting, SOW Worker, Profile Worker, Worker, Resource, Work Order, Work Order Revision, Interview, Social Enterprise Note - Erasing a resource also erases all the PII contained within the Resource Time Sheet of that resource. - Job Posting PII will be erased upon selection of the final Worker.
PII custom fields erased	Modules: SOW Worker, Profile Worker, Worker, Resource, Historical Worker, Worker Order, Worker Order Revision, Expense Sheet, Invoice, Consolidate Invoice, Miscellaneous Invoice, Credit/Debit Memo Note Erasing a resource also erases all the PII contained within the Resource Time Sheet of that resource.
Downstream records updated	The Worker/Resource Name is removed from objects such as Time Sheet, Expense Sheet, Invoice, etc.
Resume/CV deleted	The Resume/CV is removed from the Job Seeker record.
Consolidated Worker updated	The Worker Order ID is removed from the Assignment tab. The Worker Record is removed from the Related tab. Note: For Master Worker PII fields, data is erased when the last Work Order record for the Consolidated Worker is selected.
Workforce records updated	The History tab is updated to remove Job Seeker, Work Order, and Job Posting.
Activity Items with PII attachments deleted	Attachments with the PII flag enabled are removed from applicable Activity Items. Note: Attachments on the Job Seeker, Work Order, Resource (and its Resource Time Sheet), Interview, Social Enterprise or Activities (that do not have the PII flag enabled) display in the Attachment List View for review and deletion.

PII Data Erasure Action	Description
Person table records erased	Information from the person fields and PII history is removed. This erasure applies to profile workers, contingent workers, SOW workers, and resources. Note: In order for this erasure to occur, no other records can be associated to the person (from the same buyer or any other buyer in cases of multiple jobs). Additionally, the person can't be active on any work order at the time of erasure.

Attachment List View

When the Personally Identifiable Information (PII), Attachment list view is used to erase data, the attachments are scrubbed in the SAP Fieldglass application.

Attachment List View

The following tables provide SAP Fieldglass's default best practice for PII data fields that will be erased on records selected from the Attachment list view.

Attachments from the following modules are included:

- Job Posting
- Job Seeker
- Interview
- Work Order
- Work Order Revision
- Profile Worker
- Activities (that do not have the PII flag enabled)
- Time Sheet
- Expense Sheet
- Invoice
- Consolidate Invoice
- Miscellaneous Invoice
- Credit/Debit Memo
- SOW Invoice
- SOW Credit/Debit Memo
- Resource

Personally Identifiable Information Data Fields

The SAP Fieldglass fields that are considered personally identifiable information are erased when the list views are used to select records for erasure.

This table provides a list of the SAP Fieldglass native fields, by module, that are erased when a user with permission selects records to be erased on the Personally Identifiable Information (PII) list views. If you have custom fields that are flagged as PII, they will also be erased.

Module	Fields
Job Posting	• Description • Internal Description • Buyer Reference • Comments to Supplier
Job Seeker	• First Name • Last Name • Unique ID • Security ID • Job Seeker Email (when Auto Engage enabled) • Profile Picture • Resume/CV • Comments • Qualification of Certification Type w/ Require Attachment
Interview	• Job Seeker • Details • Mark As Completed Comments • Mark As No Show Comments • Accept Interview/Meeting Schedule - Step 2 Comments • Phone Number for the Interviewer
Work Order / Work Order Revision	• Buyer Reference • Comments to Buyer • Comments to Supplier • Supplier Reference • Worker Email (non-Auto Engage)
SOW Work Order / SOW Work Order Revision	• Buyer Reference • Supplier Reference • Resume/CV

Module	Fields
Worker (Contingent and SOW)	• Buyer Reference • Supplier Reference • Unique ID • Security ID • Username • First Name • Last Name • Email • Cc Email Addresses • Address 1 • Address 2 • City • State/Province • Country • Zip/Postal • Phone Number • Fax Number • Mobile Number • Public Profile URL
Profile Worker	• First Name • Last Name • Phone Number • Fax Number • Email • Address 1 • Address 2 • City • State/Province • Country • Zip/Postal • Mobile Number • Comments • Profile Picture • Buyer Reference • Unique ID • Security ID • Supplier Reference
Social Enterprise	• Annotations • Chat • Reminder

Module	Fields
Consolidated Worker	• First Name • Last Name • Phone Number • Fax Number • Mobile Number • Email • Address 1 • Address 2 • City • State/Province • Country • Zip/Postal • Security ID
Resource	• User Name • Worker Country of Origin • Security ID • Phone Number • Fax Number • Address 1 • Address 2 • City • State/Province • Country/Region • Zip / Postal Code Erasing a resource also erases all the PII contained within the Resource Time Sheet of that resource, such as the name of the resource, reference IDs, and any approver comments. Any attachments associated to resources and resource time sheets are permanently deleted.
Worker Evaluation	Comments
Absence	• Worker • Entered By • Comments
Decision Form	• Name • Creator • Owner • Decision Form Creator Email • Decision Form Owner Email • Proxy Approver Username
Decision Form with Named Resource	• First Name • Last Name • Email

1.3.3 SAP Fieldglass - Erasing Your Personal Information

This document provides guidance to workers who want to erase themselves in the SAP Fieldglass cloud service.

If you no longer want your personal information to personally identify you in the SAP Fieldglass application, you need to do the following.

Note

If you registered in a buyer's candidate portal you can delete yourself from the portal. When you are logged into the portal and access your profile, the [Delete Profile](#) button displays. When the button is selected, the application validates that there are no open records linked to the profile. If none exist and you confirm the deletion, you are logged out and your record is permanently deleted from the portal. If there are open records, you should follow the steps below. Once the records are closed and erased, you will be able to use the Delete Profile button to remove your record from the portal.

Step 1: Erase Your Profile

You control the data on your profile; therefore, you are the only one that can make changes to your profile information. Login to the SAP Fieldglass application and edit your profile. Change the information on your profile so that it no longer personally identifies you. Some fields you may want to erase on your profile include:

- Username – Change your username if it identifies you.
- Email – Change your email address (example: XXXX@anonymize.com) and remove any Cc Email addresses.
- Remove your mailing address and phone numbers.
- Remove any links to your public profile.

Step 2: Contact Your Data Controller(s)

Information that can personally identify you may exist in other areas of our cloud service beyond your profile; therefore, to complete the erasure process, additional action needs to be taken by the entities and individuals who control access to your personal information, which may be one or more supplier* or buyer* organizations that have chosen to leverage the SAP Fieldglass cloud service to help support an external workforce or services procurement program ("Data Controller"). Please note, as the "Data Processor", SAP Fieldglass can only process your data as per the legal agreement with the Data Controller. Below are the steps that need to be taken with each Data Controller:

Contact each Data Controller and inform the Data Controller of your desire to have your personal information erased. As the entity that controls access to your personal information (other than your profile), the Data Controller will need to (1) take action within the cloud service to ensure records containing your personal information are erased and (2) contact SAP Fieldglass and formally request (in writing) that SAP Fieldglass erase your name. If you are not certain who the Data Controllers are, start by contacting your supplier organization. This entity may be the company that was issuing your paycheck, was your employer of record, or has helped get you a work assignment at an organization.

*A buyer is an entity that has chosen to leverage the SAP Fieldglass cloud service to help support an external workforce or services procurement program. A supplier is a vendor who provides a buyer with workers and/or services.

Note

The information provided in this informational guide is not legal advice and should not be interpreted as such. If there are questions related to legal requirements, please seek legal counsel.

1.3.4 SAP Fieldglass - Erasing a Worker/Erasing a Supplier User

This document provides guidance to suppliers who want to erase a worker or supplier user in the SAP Fieldglass cloud service.

Erasing a Worker

Since the worker controls the data that displays on the profile, the worker is the only one who can make changes to the profile information. A worker who no longer wants to be identifiable in the SAP Fieldglass application must change the profile information. The document, [Erasing Your Personal Information in SAP Fieldglass](#), is available and can be given to workers to assist them with this.

Personally identifiable information likely exists in other areas of the cloud service beyond the worker profile; therefore, to complete worker erasure, additional action may need to be taken by other entities who control access to such personal information. These entities may be one or more supplier or buyer organizations that leverage the SAP Fieldglass cloud service to support an external workforce or services procurement program (collectively, "Joint Data Controller(s)"). As the data processor, SAP Fieldglass cannot make erasure decisions on behalf of Joint Data Controllers. Each Data Controller needs to take actions within the cloud service to erase the personal information it controls. SAP Fieldglass recommends that your organization coordinates with Joint Data Controllers to ensure all applicable personal information is erased.

When a worker contacts your organization, your organization needs to determine if it is appropriate to erase cloud service records your organization controls (e.g. workforce records). For example, a workforce record is generated in the SAP Fieldglass cloud service when a supplier submits a person as a Job Seeker. If the applicable data subject was submitted multiple times, multiple workforce records will exist for the person and each record may need to be erased.

When a workforce record is in Closed/Inactive status, supplier users with  [Workforce](#)  [Manage](#)  permission see the **Delete** button on the workforce record. When Delete is selected and confirmed, the record is permanently erased from the SAP Fieldglass cloud service and the action cannot be reversed. Attachments and the indexes used for searching are removed. The record no longer appears anywhere including:

- Custom fields
- List views
- Related tabs on other documents

- Named job postings
- Submit existing job seekers lists
- Potential match lists
- New reports (Reports that have already been run may still include the workforce record information. Stored reports are cleared after 90 days)
- New downloads (Downloads that have already been done may still include the workforce record information. Stored download data are cleared after 90 days.)
- New messages/notifications (Messages/notifications that have already been sent may still include the workforce record information.)
- Personally Identifiable Information Audit Trail

Erasing a Supplier User

Supplier organizations control what data is on a supplier user's account, which may include personal information. When it is necessary for a user to no longer be identifiable in the SAP Fieldglass cloud service, administrators and users with permission to erase closed users go to ► [Admin Configuration](#) ► [User](#) ► and choose the closed user you want to erase. Select the **Erase** button. The user is placed in Pending Erasure status for 14 days and the option to Undo Erase is available. After 14 days, the user is erased in the SAP Fieldglass cloud service. An upload is also available to erase closed users, **Standard User Data Erasure Upload**.

When a user is erased, the data is scrubbed in the following manner:

- The name and email information are replaced with 'XXXX.' Cc email addresses are blanked out.
- The Profile Picture is removed.
- The Employee ID and Contact Information is blanked out.
- User Profile fields such as Supervisors and Signature Authority are blanked out. Feature Access fields are disabled.
- The user is no longer available for selection from any modals or list views.
- If the user appeared in any document, work item, or system audit trail, their name is replaced with 'XXXX.'
- The user no longer displays in any reports.

ⓘ Note

The information provided in this informational guide is not legal advice and should not be interpreted as such. If there are questions related to your organization's legal requirements, please seek legal counsel.

1.3.5 SAP Fieldglass - Erasing a Worker/Erasing a Buyer User

This document provides guidance to buyers who want to erase a worker or buyer user in the SAP Fieldglass cloud service.

The purpose of this document is to provide buyers with information about managing the personal information of workers and users in the SAP Fieldglass cloud service. It is important to understand who controls the data.

- **Data Controllers** – The entities that determine the purposes and means of processing the personal data of a “data subject” (job seekers, workers, users). Buyers and suppliers are data controllers. Workers can also be data controllers.
- **Data Processor** – Process personal data on behalf of Data Controllers but do not control the data. SAP Fieldglass is a data processor.

When there is a need to erase personal data, SAP Fieldglass can help facilitate the request from a data processor perspective; however, the organizations and individuals who are the data controllers (buyers, suppliers, and workers) need to use the administrative functionality/tools within the SAP Fieldglass cloud service to actively remove relevant personal data.

For cases where buyers want to report on the history of changes to Personally Identifiable Information fields, the PII Audit report is available by default to users with the correct permissions.

What do you want to accomplish?

As a buyer, you should consider what you want to accomplish when managing the personal information of data subjects:

- The Managing Data Retention Policies feature should help accomplish your personal data retention requirements. See the feature overview below.
- If you want to erase an individual’s personal data which is controlled by other data controllers (e.g. suppliers and workers), there are additional actions beyond using the Managing Data Retention Policies feature that need to be considered. Refer to Erasing a Worker and Erasing a Buyer User below.

Managing Data Retention Policies Feature Overview

If your company has a data retention policy that dictates when personal data should be erased, the SAP Fieldglass feature, [Managing Data Retention Policies](#), can be enabled. This functionality is typically used to manage the personal data within a buyer’s retention policy. When enabled, thresholds are established and when the threshold has been met, the record appears on a list view and users with permission can access the list view to select the records from which personal data should be erased. Download and upload utilities are available that provide a streamlined way to manage the erasure of large volumes of job seekers, workers, and related attachments.

Additionally, this feature includes the ability for buyers to search for a worker or job seeker who has not met the established thresholds and select them for erasure.

Keep in mind that when a buyer uses this feature, there is an impact to the supplier because certain objects are visible to both buyers and suppliers; therefore, when the objects are erased, they are also erased for the supplier. For example, when a job seeker is selected to be erased, the name, resume, and association to a job posting and workforce gets erased. This means that the supplier would no longer be able to figure out who the applicant was or to what position the person was submitted. When a worker is selected to be erased, the assignment record gets erased. The supplier is no longer able to know who was on the assignment. To summarize, the following documents are impacted for suppliers:

- **Workforce:** History on Job Seeker or Worker records is removed

- Job Seeker, Worker, and Resource: Records are erased
- Time Sheet/Expense Sheet: Name is removed
- Invoice: Name is removed (if applicable)

To enable the Managing Data Retention Policies feature, SAP Fieldglass support is required. The **Managing Job Seeker, Worker, and User Privacy in SAP Fieldglass** document is available for more information about it.

The Managing Data Retention Policies feature erases personal data that is controlled by the buyer; however, it does not erase all personal data from the SAP Fieldglass cloud service. This is because some data is controlled by other organizations and individuals. For example, the worker controls the data on the worker profile and a supplier typically controls the data on a workforce record. If the worker or user needs to be erased, the information below provides guidance on erasing workers and users.

Erasing a Worker

Worker Profile

Since the worker controls the personal data that displays on the profile, the worker is the only one who can make changes to the profile information. A worker who no longer wants to be identifiable in the SAP Fieldglass cloud service must change the profile information. The document, **Erasing Your Personal Information in SAP Fieldglass**, is available and can be given to workers.

Workforce Record

If the worker needs to be totally erased, additional action may need to be taken by other entities who control access to such personal data. These entities may be one or more supplier or buyer organizations that leverage the SAP Fieldglass cloud service to support an external workforce or services procurement program (collectively, "Joint Data Controller(s)"). As the data processor, SAP Fieldglass cannot make erasure decisions on behalf of Joint Data Controllers. Each Data Controller needs to take actions within the cloud service to erase the personal data it controls. Typically, the workforce record data is controlled by the supplier. The document, **Erasing a Worker / Erasing a Supplier User**, is available and can be given to suppliers.

However, if the buyer created the workforce record, the buyer would control the workforce record. Even if the buyer is using the Managing Data Retention Policies feature, the workforce record is not erased. In this situation, the buyer would need to erase the workforce record. It is up to the buyer to determine whether it is appropriate to erase cloud service records (e.g. workforce records created by your organization). To erase the workforce record, your organization can locate the workforce record(s) and edit them to remove any personal data. Some workforce fields you may want to erase include:

- First and Last Name – Change to generic characters such as "XXXX."
- Resume/CV and Profile Picture – Remove.
- Pay Rate and Bill Rate – Enter "0."
- For any optional fields, remove any values that can identify the individual such as the contact information.
- Make other changes as desired such as removing job codes and qualifications.
- Remove any Tags.
- Close the workforce record which moves it to the Past Data list view.
- Repeat for every workforce record.

Erasing a Buyer User

Buyer organizations control what data is on a buyer user's account, which may include personal data. When you determine it is no longer necessary for a user to be identifiable in the SAP Fieldglass cloud service, administrators and users with permission to erase closed users go to ► [Admin Configuration](#) ► [User](#) ► and choose the closed user to be erased. Select the [Erase](#) button. The user is placed in Pending Erasure status for 14 days and the option to [Undo Erase](#) is available. After 14 days, the user is erased in the SAP Fieldglass cloud service. An upload is also available to erase closed users, **Standard User Data Erasure Upload**.

When a user is erased, the data is scrubbed in the following manner:

- The name and email information are replaced with 'XXXX.' Cc email addresses are blanked out.
- The Profile Picture is removed.
- The Employee ID and Contact Information is blanked out.
- User Profile fields such as Supervisors and Signature Authority are blanked out. Feature Access fields are disabled.
- The user is no longer available for selection from any modals or list views.
- If the user appeared in any document, work item, or system audit trail, their name is replaced with 'XXXX.'
- The user no longer displays in any reports.

Note

The information provided in this informational guide is not legal advice and should not be interpreted as such. If there are questions related to your organization's legal requirements, please seek legal counsel.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.

