

GDPR Readiness Program March 2024

Table of Contents

[General Data Protection Regulation (GDPR) Anonymization/Deletion 1](#_Toc161994082)

[User Record Anonymization 3](#_Toc161994083)

[User Record - Legal Entity OU 5](#_Toc161994084)

[Users Administration - Anonymized Users 6](#_Toc161994085)

[Data Load Wizard - Legal Entity OU Load 8](#_Toc161994086)

[Cornerstone HR Data Anonymization 9](#_Toc161994087)

[GDPR - Effective Dated Record Anonymization 10](#_Toc161994088)

[GDPR - Forms Anonymization 12](#_Toc161994089)

[GDPR Compliance in Planning 13](#_Toc161994090)

[Learning Data Anonymization 14](#_Toc161994091)

[Essential Transcript Data Deletion for Compliance (Early Adopter) 15](#_Toc161994092)

[Performance Data Anonymization 18](#_Toc161994093)

[GDPR - Performance Review Task Administration - Data Deletion and Anonymization 19](#_Toc161994094)

[GDPR - Performance Reviews Data Deletion and Anonymization 21](#_Toc161994095)

[GDPR - Goals Data Deletion and Anonymization 22](#_Toc161994096)

[GDPR - Competency Assessment Task Data Deletion and Anonymization 23](#_Toc161994097)

[GDPR - Observation Checklist Data Deletion and Anonymization 24](#_Toc161994098)

[GDPR - Development Plan Data Deletion and Anonymization 25](#_Toc161994099)

[GDPR - Skills Matrix Data Deletion and Anonymization 26](#_Toc161994100)

[GDPR - Feedback Data Deletion and Anonymization 27](#_Toc161994101)

[GDPR - Succession Planning Administration - Data Deletion and Anonymization 28](#_Toc161994102)

[GDPR - Succession Planning Task Data Deletion and Anonymization 29](#_Toc161994103)

[GDPR - Evergreen Succession Data Deletion and Anonymization 30](#_Toc161994104)

[GDPR - Talent Pools Data Deletion and Anonymization 31](#_Toc161994105)

[GDPR - Universal Profile Data Deletion and Anonymization 32](#_Toc161994106)

[Recruiting Data Anonymization 33](#_Toc161994107)

[Data Deletion to Support Data Privacy for Recruiting 34](#_Toc161994108)

[GDPR - Compliance Enablement Preferences - Applicants Settings 39](#_Toc161994109)

[GDPR - Deletion of Applications 40](#_Toc161994110)

[GDPR - Anonymization by User 43](#_Toc161994111)

[GDPR - Ad Hoc Anonymization 45](#_Toc161994112)

General Data Protection Regulation (GDPR) Anonymization/Deletion

Cornerstone clients, particularly in the European Union, require the ability to anonymize/delete data associated with a user to ensure compliance with local and federal regulatory requirements, among which General Data Protection Regulation (GDPR) is the most prominent change. This can also have an impact on non-European clients with users in Europe who are covered by the related regulations.

For internal users, organizations can request that employee data be made anonymous based on the following removal scenarios:

* User Based Removal - For non-applicant users, this type of anonymization occurs when requested by a client. This type of removal is not dependent on the user's status or Legal Entity. When this type of removal, if the user is Inactive, the user record is anonymized and peripheral data is deleted; if the user is Active, the user record is not impacted but the peripheral data is deleted.
* Time Based Removal - This type of anonymization occurs automatically after a certain period of time. All internal users (not applicants) must be Inactive to be anonymized. For this type of removal, the user does need to have a Termination Date populated, and the user must belong to a Legal Entity. The Legal Entity determines the user record retention period.

* Peripheral Data - Organizations can set criteria for the deletion of peripheral data, such as performance reviews, development plans, etc. This deletion may occur before a user is anonymized, and it may occur regardless of the user's status (i.e., Active, Inactive) and employment status (e.g., Terminated).

Notes:

* If the retention period is set up only for user record, ONLY user data is anonymized/deleted when the user is made inactive and the retention period has passed. Peripheral data remains in the system.
* If the retention period is also set up for peripheral data (performance review, goals, competencies, etc.), the user's peripheral data is deleted regardless of the termination date and user status (i.e., Active, Inactive). This means that peripheral data deletion may occur before a user is anonymized.

For applicants, organizations can request that applicant data be made anonymous based on the following removal scenarios:

* As a part of deletion of individual applications, a user's application will be deleted when the following has occurred:
	+ The requisition is closed or the user is in a closed status
	+ The non-hired application in that closed requisition has exceeded the retention period as defined per the Location Organizational Unit (OU) (primary location) of that requisition
	+ A user has left a legal entity, becomes inactive, and either requests to be forgotten OR whose data has exceeded the retention period for that Location OU of the closed requisition or exceeded the retention period for the Legal Entity (whichever comes first)
	+ An applicant requests from the administrator that their application be deleted at any given point in time (whether or not the application has exceeded the data retention period of a closed requisition)
* As a part of anonymization, a user’s information will be anonymized when the following has occurred:
	+ The applicant has exceeded the period of inactivity as defined by the administrator in the Compliance Enablement Preferences area and that applicant has been dispositioned from a requisition

There are two types of data removal:

* Deletion - Data deletion removes the data from all databases, and the data is not recoverable.
* Anonymization - Data anonymization scrambles the user's identifiable information, and this process is not reversible.

Data removal can be configured based on a standard organizational unit (OU), Legal Entity. The Legal Entity OU can only be used for data removal.

Considerations

Although Learning and other product suites are not explicitly mentioned in this documentation, all suites are impacted by data anonymization. For example, Learning records will remain available when a user is anonymized, but the records are not identifiable.

Implementation

Except for applicant anonymization, this functionality is controlled by a backend setting that is disabled by default.

To enable this feature please first speak with your Account Manager or Client Executive as we offer different enablement paths depending on the complexity of your requirements. Once requirements are defined, submit a work order to Global Customer Support to enable the data retention rules for Legal Entity and Location OUs.

Map Data Retention to Legal Entity/Location OU

To define the data retention rules for Legal Entity and Location OUs, you must submit a work order to Global Customer Support.

User Record Anonymization

After a user record is anonymized, certain fields are anonymized and other fields are deleted. Also, the Modification History section does not show any identifiable information.

When editing a user record that has been anonymized, changes cannot be saved. A message is displayed at the top of the user record to indicate that the user record has been anonymized and can no longer be edited.

A user record can only be anonymized if their status is Inactive.



When a user record is anonymized, the following information is anonymized:

* Prefix
* First Name
* Middle Name
* Last Name
* Suffix
* Username
* User ID
* Local System ID
* Original Hire Date - This is set to 1/1/1901
* Last Hire Date - This is set to 1/1/1901
* Address Line 1
* Address Line 2
* City
* State

When a user record is anonymized, the following information is deleted:

* User Photo
* Country
* Email Address
* Personal Email Address
* Zip
* Phone
* Fax
* Mobile Phone
* Employee Relationships (e.g., Manager, Approver)
* Custom Fields

For organizations using the fields below, the following information is also deleted:

* User Type and Sub Type
* Employment Status
* Leave Type
* Termination Reason
* Termination Date
* Termination Type
* Eligible for Rehire
* Rehired Employee
* For Sensitive Personally Identifiable Information (SPII) fields present in the Data Load Wizard and reporting that do not display on the user record, the values are deleted.

When a user record is anonymized, the following information is not impacted:

* Organizational Units (e.g., Division, Position, Grade)

User Record - Legal Entity OU

When Data Deletion is enabled, a new Legal Entity organizational unit (OU) is available on the user record. The Legal Entity OU is used when configuring Data Deletion Preferences. With the exception of applicant data, data deletion preferences can only be configured by Cornerstone.

Users Administration - Anonymized Users

When a user has been anonymized, the user record is still available in the Users Administration area, and the user appears when searching for users. However, the user's information is anonymized in the search results.

To access the User Records Administration page, go to Admin > Tools > Core Functions > Users.

Permissions

|  |  |  |
| --- | --- | --- |
| PERMISSION NAME | PERMISSION DESCRIPTION | CATEGORY |

|  |  |  |
| --- | --- | --- |
| Users - View | Grants the ability to search for and view summary information about users in the portal via the Admin/Users screen. This permission can be constrained by OU, User's OU, User Self and Subordinates, and Users. If multiple constraints are added, these constraints are considered OR statements. This is an administrator permission. | Core Administration |

|  |  |  |
| --- | --- | --- |
| Users - View Core and Edit Custom Fields | Grants ability to view core information on a user record, including first name, last name, username, assigned OUs, custom relationships, and custom fields. This permission also includes the ability to edit any custom fields that are visible to the administrator. This permission works in conjunction with the Users - View permission. This permission can be constrained by OU, User's OU, User Self and Subordinates, and User. This is an administrator permission.Note: When the User Record Redesign is enabled in a portal, this permission is disabled. Administrators who previously had this permission are automatically assigned the following permissions:* Universal Profile - User Record - Edit Users
* Universal Profile - User Record - View Users
* Users - Edit Custom Field Information
* Users - View Custom Field Information
* Users - View General Information

This permission is obsolete following the retirement of the legacy User Record in the May '17 release. | Core Administration |

|  |  |  |
| --- | --- | --- |
| Users - View Criteria Search | Enables those who can search for and view users via the Admin/User screen to search by OU and Group criteria. This permission only works when assigned in conjunction with the Users - View permission. | Core Administration |

|  |  |  |
| --- | --- | --- |
| Users - View Manager Search | Enables those who can search for and view users via the Admin/User screen to search by users' assigned manager. This permission only works when assigned in conjunction with the Users - View permission. | Core Administration |

Data Load Wizard - Legal Entity OU Load

To support the Legal Entity organizational unit, a Legal Entity OU load is available. This data load enables administrators to load Legal Entity OU data into the system.

In addition, the Users data load enables administrators to associate users with a Legal Entity OU.

Cornerstone HR Data Anonymization

GDPR - Effective Dated Record Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, effective dated records are anonymized. When an effective dated record is anonymized, certain fields are anonymized and other fields are deleted.

When an effective dated record is anonymized, the following information is anonymized:

* Prefix
* First Name
* Middle Name
* Last Name
* Suffix
* Username
* User ID
* Local System ID
* Original Hire Date - This is set to 1/1/1901
* Last Hire Date - This is set to 1/1/1901
* Address Line 1
* Address Line 2
* City
* State
* Zip
* Country
* Time Zone
* Phone
* Fax
* Mobile Phone
* Signature
* User Status
* Relationships
* Allow Reconciliation

When a user record is anonymized, the following information is deleted:

* Email Address
* Personal Email Address
* Absent Status
* User Type and Sub Type
* Employment Status
* Leave Type
* Termination Reason
* Termination Date
* Termination Type
* Eligible for Rehire
* Rehired Employee
* Custom Fields
* For Sensitive Personally Identifiable Information (SPII) fields present in the Data Load Wizard and reporting that do not display on the user record, the values are deleted.

When a user record is anonymized, the following information is not impacted:

* Organizational Units (e.g., Division, Position, Grade)
* Display Language

Note: To enable instant application data deletion and profile anonymization, contact GCS.

GDPR - Forms Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, all forms related to the user are deleted.

When the anonymized user is the subject of the form, the following occurs:

* The form is deleted from Snapshot Documents, including all attachments.
* Any tasks related to the form are deleted from the Actions tab within Actions.
* Any open form that is not completed or completed but not approved are deleted.

When the anonymized user is a manager, the following occurs:

* Any form tasks in the manager's Actions tab are deleted.

When the anonymized user is an approver, the following occurs:

* Pending approvals are removed from the approver's Requests tab.

GDPR Compliance in Planning

Headcount Planning is compliant with GDPR by automatically scanning and anonymizing relevant user data.

Prior to compliance, Headcount Planning did not have anonymization or data deletion functionality and was not able to remove user data as required by GDPR. The Planning application can now allow clients to remove user data, as required by GDPR.

Anonymization Notes

The process for anonymizing data will be as follows:

1. The data that is anonymized is the User First Name and User Last Name.
2. The system User ID can be retained, but any user ID that has been shown to users in the Planning application.
3. Position attributes, such as Country, can be retained because they are attached to the Position-seat and not the user.
4. The user names associated with subplan comments are anonymized, but the comments themselves are not deleted or anonymized.

Reporting

When reporting on Planning data, incumbent names for users who were anonymized are not included in the export of the Planning data.

Implementation

For portals using Headcount Planning, this functionality is automatically enabled.

Note: Headcount Planning is available by request at an additional cost. Contact your Client Executive for additional information.

Learning Data Anonymization

Essential Transcript Data Deletion for Compliance (Early Adopter)

Essential Transcript Data Deletion provides organizations the ability to automatically delete User Transcript Data based on a defined retention period for inactive users in accordance with various regulations, such the EU GDPR and the Right to be Forgotten policy.

Important: To enable this enhancement, contact Global Customer Support.

Once enabled, administrators can activate this feature by going to Admin > Tools > Learning > Learning Preferences > Feature Activation Preferences. In the Feature Activation section, for the Activate Learning Transcript Deletion Mechanism for Compliance area, click the Activate button. The following applies once activated:

* Data deletion respects the retention rule set at the Legal Entity Organizational Unit (OU) which users are part of at the time of the deletion.
* Automatic deletion applies to the transcript of inactive users who are terminated.

Deleted Data

The following Essential Transcript Data is deleted:

| Transcript Peripheral Data | Transcript Core Data |
| --- | --- |
| Training Certificates​ ​ | Transcript data for the transcript of the User (LO id, LO Title, subject, version etc.)​ |
| ​ Attachments (OJT/ Express Class)​  |  Transcript status (not started, pending approval, in progress, completed, etc.) and eventual scores​ |
|  Comments (entered when assigning, approving/ denying, marking complete, updating transcript, exempting, removing, etc.)​  | Dates (assignment date, due date, completion date, etc.)​  |
|  Evaluations | ​ Active, Completed, Archived , Removed Transcript |
|  Reporting |   |

 Time-based Data Deletion

The following applies to time-based data deletion:

* Time-based deletion occurs automatically after a certain period. The execution itself is triggered on daily basis for Inactive User’s Learning Transcript Data based on the User’s termination date.
* The user must belong to a Legal Entity OU and must be inactive. Users should be assigned to the Legal Entity before their termination date.
* Data is erased permanently from the database and cannot be recovered. Data is also removed from the Reports.
* Customers must enable User data anonymization/ deletion prior to Time based activation for Transcript for each Legal Entity OU.
* Before opting-in for this process Customers must request via GCS one-time historical data cleanup for previously anonymized/ deleted users if they already use User anonymization/ deletion mechanism in their portal. ​

Frequently Asked Questions (FAQs)

Q: Do we need to perform a copy down to stage before enabling the feature for testing?​

A: Yes, it’s a best practice to perform copy down to stage before enabling the new feature in the stage portal for testing on the most updated data available in the Production portal.​

Q: Will Transcript Deletion preserve statistics?​

A: No, deletion does not preserve statistics.

Q: Will Transcript Data related to xAPI be deleted?​

A: Yes, only xAPI records on the User transcript level would be deleted. Data under xAPI statement viewer/ LRS is out of scope of this release.​

**Q: Do we need to enable User Data anonymization/ deletion before Transcript?​**

A: Yes, it is mandatory to enable User Data anonymization/ deletion configuration with Legal Entity OUs/ settings/ retention period before opting for the time-based Transcript Data Deletion.​

Q: Do we need to perform historical transcript data deletion for previously anonymized users prior to time-based transcript data activation?​

A: Yes, it is mandatory to perform this one-time activity to avoid load on the system for first time enablement.

**Q: Is it possible to restore data that has been deleted through the transcript data deletion functionality?**

A: No, the purpose of deletion is that the data is gone, and Customers nor Cornerstone longer process or possess a person’s transcript data. Be very careful and diligent when choosing retention periods, and to do proper UAT before deploying in production.​

Q: What is the process for Customer to opt for automated time-based transcript data deletion?​

A: First, the Customer must activate user data anonymization/ deletion mechanism, if already leveraging. Next, request historical data cleanup for previously anonymized users via GCS case/ work order. Finally, request the enablement of the feature activation preference visibility on the UI in the same case to toggle the preference for time-based.​

**Q: What will happen to the User Transcript and other screens post the data is deleted?​**

A: User's will have an empty transcript with data deleted from active, completed, archived and removed tabs as well as relevant reports and system areas like Session Roster Page, Curriculum Administration > View Users, etc.

Q: What happens if a person (by error) belongs to multiple Legal Entity OUs at the same time?​

A: Transcript data generated during an overlapped Legal Entity window will have both Legal Entity tags associated and will be deleted based on the shortest retention period​

**Q: What happens if there is API Integration in place for Transcript Data?​**

A: API only returns transcript data for active users.​

Implementation

This functionality is off by default. Contact Global Customer Support to enable.

Performance Data Anonymization

GDPR - Performance Review Task Administration - Data Deletion and Anonymization

When an administrator who has created a performance review task leaves a Legal Entity organizational unit (OU) and requests to be forgotten, their name is anonymized in the Created By column on the Performance Review Task Administration page.

To access Performance Review Task Administration, go to Admin > Tools > Performance Management > Tasks.

Permissions

|  |  |  |
| --- | --- | --- |
| PERMISSION NAME | PERMISSION DESCRIPTION | CATEGORY |

|  |  |  |
| --- | --- | --- |
| Performance Review Task Administration | Grants ability to create/assign performance review tasks and manage activity within those tasks. This permission also gives the ability to enable and view co-planners for a task from the administration pages. This permission can be constrained by OU, User's OU, User Self and Subordinates, and User. | Performance - Administration |

|  |  |  |
| --- | --- | --- |
| Task - View | Grants ability to view assigned tasks via Scheduled Tasks screen and Welcome Page My Tasks widget. This is an end user permission. | Core |

|  |  |  |
| --- | --- | --- |
| View Performance Reviews | Grants ability to view the Performance Reviews page, which displays a user's own past performance reviews as well as performance review task steps they've been assigned to complete. This also grants ability to view the Batch Rating page. This permission can be constrained by OU, User's OU, User Self and Subordinates, and User. This is an end user permission. | Performance |



GDPR - Performance Reviews Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, performance reviews are impacted in the following ways:

* Reviewee - If the user is a reviewee, the user's performance review and any underlying Form Sections are deleted.
* Reviewer - If the user is a reviewer, the user's core data such as First Name and Last Name are anonymized, such as in areas of the performance review PDF. That is, the reviewee's scores and comments remain intact, but any references to the reviewer are anonymized. This includes if the reviewer is a peer reviewer or a co-planner.
	+ Sign-off Section - In the Sign-off section, the review's signature is anonymized.
* Administrator - If the user is an administrator, the user's core data such as First Name and Last Name are anonymized throughout Performance Review Task Administration.

When a data deletion request is made based on time, the performance review task end date is used to determine when the data is deleted or anonymized.

GDPR - Goals Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, goals are impacted in the following ways:

* Individual Goals - If the user is the Goal Owner, the goal is deleted.
* Shared Goals - If the user is the Goal Owner of a shared goal, the goal is deleted.
* Manager Comments - If the user is a manager who has added comments to a subordinate's goal, the manager's core data such as First Name, Last Name, and Email Address are anonymized. That is, the comments remain intact, but any references to the manager are anonymized.

When a data deletion request is made based on time, the goal due date is used to determine when the data is deleted or anonymized. If the goal does not have a due date, then the goal creation date is used.

Considerations for Goals:

* When a user requests to be forgotten OR that user’s data is outside of the data retention period and that user has created a Feedback request, then any goals that are used in the Feedback Requests are not deleted since the Feedback Request uses a snapshot of the goal from when the request is made. A best practice for administrators is to request the deletion of both Goal and Feedback Requests.

* When a user requests to be forgotten OR that user’s data is outside of the data retention period and that user has goals within a Goal Rating or Goal Planning section of a Completed or Expired performance review, then those goals are not deleted because the goals reflected in these sections are snapshots of the goals. A best practice for administrators is to request the deletion of both Goal and Performance Review data.
* If an owner of a shared goal is leaving a legal entity, a best practice is to reassign the shared goal prior to making a data deletion request. This can be done from the Goals Edit page or the Manage Shared and Dynamic Goals page. The owner can re-assign the goal in the Managed by section.

GDPR - Competency Assessment Task Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, competency assessment tasks are impacted in the following ways:

* Assessee - If the user is an assessee, the user's competency assessment is deleted.
* Assessor - If the user is an assessor, the user's core data such as First Name and Last Name are anonymized. That is, the assessor's scores and comments remain intact, but any references to the assessor's core data are anonymized.
* Administrator - If the user is an administrator, the user's core data such as First Name and Last Name are anonymized throughout Competency Task Administration.

When a data deletion request is made based on time, then the competency assessment task end date is used to determine when the task data is deleted or anonymized. The last modified date is used to determine when competency ratings are deleted.

GDPR - Observation Checklist Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, observation checklists are impacted in the following ways:

* Assessee - If the user is an assessee, the user's observation checklist is deleted.
* Validator/Verifier - If the user is a validator or verifier, the user's core data such as First Name and Last Name are anonymized. That is, the validator or verifier's validations remain intact, but any references to the validator/verifier are anonymized.
* Validator/Verifier Electronic Signature - If the user is a validator or verifier, and they have provided an electronic signature for an observation checklist, then the electronic signature is anonymized.
* Administrator - If the user is an administrator, the user's core data such as First Name and Last Name are anonymized throughout Observation Checklist Administration.

When a data deletion request is made based on time, then the checklist completion date is used to determine when the data is deleted or anonymized. If the checklist is not yet complete, then the assignment date is used.

Considerations for Observation Checklists:

* With this phase, a user's LO-based observation checklists are not deleted when the user is anonymized. LO-based checklists that are within a curriculum will be deleted as part of a future release.

GDPR - Development Plan Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, development plans are impacted in the following ways:

* Individual Development Plans - If the user is the Development Plan Owner, the development plan is deleted. This includes if the user creates a development plan or is assigned a development plan.
* Development Plan Creator - If the user is a manager or administrator who created a development plan for another user, the user's core data such as First Name and Last Name is anonymized in the History section. This includes the Development Plan PDF.
* Development Plan Comments - If the user is a manager or administrator who has added comments to another user's development plan, the manager or administrator's core data such as First Name and Last Name is anonymized in the Comment section. This includes the Development Plan PDF. That is, the comments remain intact, but any references to the user are anonymized.
* Development Plan Templates - If the user has created a Development Plan Template, the development plan template is deleted.

When a data deletion request is made based on time, the development plan completion date is used to determine when the data is deleted or anonymized. If the development plan is not complete, then the development plan creation date is used.

GDPR - Skills Matrix Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, roles are impacted in the following ways:

* Roles - If the user created a role or modified a role, the user's core data such as First Name and Last name are anonymized in the Role's Modification History and on the Manage Roles page.

GDPR - Feedback Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, feedback is impacted in the following ways:

* Feedback Request - If the user has requested feedback, then the feedback request and any responses and ratings are deleted.
	+ When a data deletion request is made based on time, then the feedback request date is used to determine when the data is deleted.
* Feedback Responder - If the user has replied to a feedback request for another user, user's core data such as First Name and Last Name are anonymized. That is, the responder's ratings and comments remain intact, but any references to the responder are anonymized.
	+ When a data deletion request is made based on time, then the feedback post date is used to determine when the data is anonymized.
* Unsolicited Feedback Post - If the user has received unsolicited feedback or a badge from another user, then the unsolicited feedback and any responses to the post for that recipient are deleted. If the user has provided unsolicited feedback for another user, then the user's core data such as First Name and Last Name are anonymized. That is, the user's feedback remains intact, but any references to the user are anonymized.
	+ When a data deletion request is made based on time, then the feedback post date is used to determine when the data is deleted.

GDPR - Succession Planning Administration - Data Deletion and Anonymization

When an administrator leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, Succession Planning Administration is impacted in the following ways:

* Template Creator - If the user created a succession planning template, then any references to their Core data such as First Name and Last Name are anonymized.
* Task Creator - If the user created a succession planning task, then any references to their Core data such as First Name and Last Name are anonymized.
* Task User - If the user is a user within a succession planning task, then any references to their Core data such as First Name and Last Name are anonymized.
* Co-Planner - If the user is a co-planner for a succession planning task, then any references to their Core data such as First Name and Last Name are anonymized.

When a data deletion request is made based on time, the following criteria is used to determine when data should be deleted or anonymized:

* Succession Task - For a succession task, the task expiration date determines when a user should be anonymized within the task.

GDPR - Succession Planning Task Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, succession planning tasks are impacted in the following ways:

* Assessor - If the user is an assessor, then any references to their Core data such as First Name and Last Name are anonymized.
* Co-Planner - If the user is a co-planner, then any references to their Core data such as First Name and Last Name are anonymized.
* Task Reviewer - If the user is a task reviewer, then any references to their Core data such as First Name and Last Name are anonymized.
* Talent Conference Reviewer - If the user is a talent conference reviewer, then any references to their Core data such as First Name and Last Name are anonymized.
* Assessee - If the user is an assessee in a Manager, Assessor, and Talent Conference tasks, the assessee is deleted from the task. In addition, any ratings, successors, or modification history associated with the assessee are also deleted.
* Position Incumbent Rating - If the user is a position incumbent in a Job Pool task, then any references to their Core data such as First and Last Name are anonymized. Also, the position incumbent ratings are deleted.
* Position Successor - If the user is a position successor in a Job Pool task, then the successor and any ratings associated with the successor are deleted.

GDPR - Evergreen Succession Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, evergreen succession data is impacted in the following ways:

* Employee Rating - All the user's evergreen ratings are deleted.
* My User Based Successor - All successors that have been named for the user are deleted.
* My Position Successor - Successors that have been named for the user's position are not affected.
* User Based Successor - The user is deleted as a successor for all users.
* Position Based Successor - The user is deleted as a successor for all positions.
* Modification History of Position Successors - Any modification history associated with the user's position successors is deleted.
* Modification History of User Successors - Any modification history associated with the user's successors is deleted.

When a data deletion request is made based on time, then the field's modification date is used to determine when the data is deleted.

GDPR - Talent Pools Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, Talent Pool succession data is impacted in the following ways:

* Talent Pool Creator - If the user has created a talent pool, then any references to their Core data such as First Name and Last Name are anonymized.
* Talent Pool Candidate - If the user has been added to a talent pool, the user is deleted from the talent pool.
* Nomination List Candidate - If the user has been nominated as a candidate for a talent pool, the user is deleted from the nomination list.
* Modification History - Any modification history associated with the user within the talent pool is deleted.

When a data deletion request is made based on time, then the last modified date of the talent pool candidate within the talent pool is used to determine when the data is deleted.

GDPR - Universal Profile Data Deletion and Anonymization

When a user leaves a Legal Entity organizational unit (OU) and requests to be forgotten OR that user’s data is outside of the data retention period, Universal Profile is impacted in the following ways:

Universal Profile - Bio:

* Resume - All the user's Bio: Resume data is deleted.
* Career Preferences - All the user's Bio: Career data is deleted.
* Job Interests - All the user's Bio: Career - Job Interest data is deleted.

Universal Profile - Snapshot:

* Goals - The Goal Progress widget is updated to reflect goals that have been deleted as a part of data deletion requests.

* Performance Reviews - The Performance Review widget scores are updated to reflect performance reviews that have been deleted as a part of data deletion requests.
* Competencies - The Competency Rating widget scores are updated to reflect competency assessment tasks that have been deleted as a part of data deletion requests.
* Badges - The Badges widget is updated to reflect badges that have been deleted as a part of data deletion requests.
* Succession:
	+ Employee Succession Ratings are updated to reflect that evergreen succession ratings have been deleted as a part of data deletion requests.
	+ User Based Successors are deleted to reflect that user’s successors have been deleted in evergreen succession as a part of data deletion requests.
	+ User is deleted as Position Based Successor for all positions as a part of data deletion requests.
	+ User’s Position Based Successors are not affected.
* Documents - All documents uploaded by the user are removed as a part of user anonymization.

Note: A user's peripheral data, such as Resume data, is only deleted if the user is anonymized.

Recruiting Data Anonymization

Data Deletion to Support Data Privacy for Recruiting

The Data Deletion project ensures that user application data is not kept in the system longer than the defined amount of time set by the data retention period. As a part of this project, Data Deletion is divided into two areas:

* Deletion of individual applications within a requisition
* Anonymization

With this functionality, you can do the following:

* Data Retention Mapping - Map data retention periods to a Location Organizational Unit (OU). This is done by the administrator through submission of a work order to Global Customer Support.
* Delete Hired Employee Data - Delete applications for hired employees who leave the Legal Entity, become inactive and who request to be forgotten OR whose data exceeds the data retention period.
* Delete Application within a Closed Requisition - Trigger the data deletion time-based event for closed requisitions.
* Data Anonymization - Applicants who have exceeded the period of inactivity for anonymization will not be dispositioned if that applicant is not dispositioned and part of a requisition that is in an Open status. In addition, the word "Archive" (or variations of it) has been replaced with Anonymization (or variations of it) in many instances throughout the system. The anonymized user is no longer searchable.

Difference between Anonymization and Deletion

* Deletion - Upon successful execution of data deletion, all non-hired applications within the Cornerstone system that have exceeded the data retention as configured by the administrator for a given Location OU, will be deleted. This deletion is permanent and non-reversible.
	+ Removal method is dependent on the scenario:
	+ For time-based: Deletion of non-hired applications based on a data retention period which is triggered following a pre-defined timeframe when the requisition is closed or the applicant is dispositioned.
* Anonymization - Replacement of applicant core user data (Prefix, Suffix, First, Middle, Last Name, Email Address, City, State, Zip, Country) with randomized string of characters within the database
	+ User of the Cornerstone system – When a user leaves a legal entity and requests to be forgotten or their core data is outside the entity’s data retention period, then that user’s core data is anonymized throughout the Cornerstone portal (e.g. Recruiter and/or Recruiting Administrator).

Note: The Compliance Enablement Preference for New Submission Anonymization is different than the anonymization described above. When the Anonymize personal applicant data for New Submissions option is selected in Compliance Enablement Preferences for a Location OU, the value in the Name column for applicants in a New Submission status is replaced with the applicant's requisition number and applicant ID. The applicant ID is scrambled so that the applicant remains anonymous. Users can still sort the table using the Name column. However, once that applicant moves into a new status, their information is no longer anonymized.

*Note:* To enable instant application data deletion and profile anonymization, contact Global Customer Support*.*

Use Cases

Use Case 1: Caitlin, the Recruiter

Date Created: 1 January 2015

Primary location of requisition: Italy

Data Retention Period: 6 months

Background:

* 35 applicants apply to the position
* 10 candidates are dispositioned
* One candidate is hired and the requisition is closed (remaining candidates are dispositioned)

Result:

* 34 remaining non-hired applications are deleted when the data exceeds the data retention period



Note: In this scenario, the hired applicant’s application will become part of the user record and will be deleted based on user deletion rules. This includes deletion upon the user leaving the entity and requesting to be forgotten or their data exceeding the defined data retention for that legal entity.

Use Case 2: Martha the recruiter defines the period of inactivity for 2 months and Jamie the applicant applies to a position

Date Created: 1 March 2015

Primary Location of Requisition: Germany

Period of Inactivity: 2 months (if applicant does not log back into Career Site, then their applicant core data is anonymized due to inactivity)

Background:

* Jamie applies to the role on 1 March (Jamie’s applied to only one requisition) and does not log back into the career site
* Jamie is dispositioned from the requisition on 1 April 2015

Result:

* Jamie’s information is anonymized due to inactivity and her dispositioned application
* Her information will not be available in Talent Pools or Saved Search



Use Case 3: Tim, the hired applicant

Company: Palmer Inc.

Legal Entity: Sweden

Data Retention Period: 2 years

Background:

* Tim applies to an application and gets hired
* Tim’s application resides with him as a user upon getting hired

Result:

* When Tim leaves the Legal Entity, the application will be deleted when it is has exceeded the data retention period



Use Case 4: Sam wants to provide information through Connect with Us for ABC Co.

Background:

* ABC Co’s period of inactivity preference is configured to 1 year after applicant submits their information
* Sam submits information through ABC Co’s Connect with Us feature on 1 Jan 2015

Result:

* Sam’s personal information is anonymized on 2 Jan 2016



Considerations

* The user's application is not deleted when moving from one Legal entity to another, provided that the user is in an Active status in the portal.
* Applications from an external source are not impacted.
* Even if a candidate exceeds the period of inactivity for a given requisition, an applicant's data is not anonymized if the applicant has an application in a job requisition that is in an Open status. However, if the applicant is dispositioned in an Open requisition for which they are the only applicant, then their data is anonymized.
* When a requisition has multiple locations, the data deletion rules will apply to the primary location of that requisition.
* If an applicant is hired, then their application will not be deleted until the user leaves the Legal Entity and either requests to be forgotten or their data exceeds the data retention period.

GDPR - Compliance Enablement Preferences - Applicants Settings

The Applicants section of Compliance Enablement Preferences allows administrators to define the settings for anonymizing applicants by defining a period of inactivity, after which time the applicant's profile is anonymized. The Applicants section also enables administrators to set personal applicant data as anonymous for new submissions and allow external applicants to deactivate their own profile.

The Applicants section of the Compliance Enablement Preferences topic contains details about each available option, including exceptions and use cases. See Compliance Enablement Preferences.

Note: Former employees cannot self-anonymize from the career site. This covers use cases in which a former employee may have been added as an employee in another way, such as through a data load. The ability to self-anonymize is controlled by the Allow applicants to anonymize their own profiles option in Compliance Enablement Preferences; however, there is no preference that controls this specific former employee use case. Data deletion features based on retention period may still anonymize this data.

Note: To enable instant application data deletion and profile anonymization, contact Global Customer Support.

To access Compliance Enablement Preferences, go to Admin > Tools > Recruit > Compliance Enablement.

Permissions

|  |  |  |
| --- | --- | --- |
| PERMISSION NAME | PERMISSION DESCRIPTION | CATEGORY |

|  |  |  |
| --- | --- | --- |
| Compliance Enablement Preferences - Manage | Grants ability to access and manage Compliance Enablement Preferences. This permission can be constrained by OU and User's OU. This is an administrator permission. | Recruiting Administration |

GDPR - Deletion of Applications

The GDPR compliance features for Recruiting are divided into the following main components:

* Anonymization of Applicant Data - Applicant data will be anonymized based on recruiting compliance configurations in the admin portal.
* Data Deletion of Internal User Profiles - User data will be anonymized and deleted based on configurations done in Core data via Global Customer Support. Global Customer Support uses the Legal Entity OU to manage different durations of time.
* Data Deletion of Applications - Application data will be deleted based on configurations done via Global Customer Support. This impacts the deletion of both internal employee and external applicant applications. Global Customer Support uses the Location OU to manage different durations of time.

Note: To enable instant application data deletion and profile anonymization, contact Global Customer Support.

Data Deletion of Applications

The time-based application data deletion scheme impacts both internal and external applicants. The retention period is configured by the Location OU (the trigger is based on the primary location of a requisition).

The trigger for the deletion is the first event happening by any of the following events:

* For applicants that are not hired, either the closing of the requisition or the disposition of the applicant.
* For applicants that are hired, changing the applicant status to Hired. Organizations can define a retention period for hired candidate application data. To set the retention period for hired application data, submit a case to Global Customer Support.

From this time, the clock starts ticking. When the retention period defined for the Location OU is reached, the application data is deleted.

For candidates in an active status in a Canceled requisition, candidate data is deleted based on the retention period and when the requisition was canceled. This will delete the applications only and not the user record. The candidates will still be searchable, but the applications will be deleted.

Applicants' inactivity does not matter for the deletion of their requisition data. In the case a client has anonymization AND Application data deletion configured, the applicant's profile can be anonymized and their application information will be deleted. It is possible, based on client configuration, that both events happen at different points in time.

Impacted Data

When either the application data deletion or user based data deletion event is triggered, all data for the user’s application is permanently deleted and will no longer be recoverable in the database. The following data will be deleted:

* Comments
* Ratings
* History / Audits
* Interviews
* Offer Letters
* Reviewers
* Selection Responses
* Realistic Job Preview
* Selection Assessment
* Skills Test
* Workflow Responses
* Competency Assessment Task
* Disclaimer
* EEO Question
* Training
* Custom Integrations
* Pre-Screening Responses
* Emails
* New Forms
* External Assessments
* Background Checks
* Attachments
* Flags
* Referrals / Costs
* Applicant Resume

When user based data deletion occurs, the above data points are deleted for ALL requisitions. In the case of only requisition data deletion occurs, the above data for only that specific requisition is deleted.

Implementation

This functionality is controlled by a backend setting that is disabled by default.

Request process: Global Customer Support work order submitted by client administrator in order to conduct the following:

1. Scheduled: One-time work order to define data deletion rules to Location OUs. Any new child locations will not dynamically inherit the data retention rules for its parent’s. If new Locations are created in the portal and retention preferences are needed to be set up for those please request this to Global Customer Support.
	1. This should be identified across all Parent Location OUs
	2. Frequency (e.g., Monthly / Annual)
	3. Day / Date (e.g., 15th of the month)
	4. Specify Retention period (e.g., 12 months)
2. Applications - Day 1 of the retention period begins one day after the requisition is closed

The organization's named administrators who can submit a Global Customer Support work order will have the ability to make modifications to the data deletion configuration. It is the client’s responsibility to ensure the named administrators will adhere to the company data deletion policy and do not make modification without discussing with the client’s data security.

When the data deletion event is triggered, all data for the applicant is permanently deleted and will no longer be recoverable and will not be available in the database. The following data will be deleted:

* General Applicant Information
* Comments
* Ratings
* History / Audits
* Interviews
* Offer Letters
* Reviewers
* Selection Responses
	+ Realistic Job Preview
	+ Selection Assessment
	+ Skills Test
* Workflow Responses
	+ Competency Assessment Task
	+ Disclaimer
	+ EEO Question
	+ Training
	+ Custom Integrations
	+ Pre-Screening Responses
* Emails
* New Forms
* External Assessments
* Background Checks
* Attachments
* Flags
* Referrals / Costs
* Applicant Resume
* Hired applications for users who leave the Legal Entity, become inactive and data has exceeded the data retention period
* Applications on an ad-hoc basis through submission of a Global Customer Support work order

Note: If an application has been submitted through an Agency and that application is subject to time-based deletion and is deleted, then the actual Agency submission should be accurately reflected in Reporting.

Note: When a requisition has multiple locations, the data deletion rules will apply to the primary location.

GDPR - Anonymization by User

The GDPR compliance features for Recruiting are divided into the following main components:

* Anonymization of Applicant Data - Applicant data will be anonymized based on recruiting compliance configurations in the admin portal.
* Data Deletion of Internal User Profiles - User data will be anonymized and deleted based on configurations done in Core data via Global Customer Support. Global Customer Support uses the Legal Entity OU to manage different durations of time.
* Data Deletion of Applications - Application data will be deleted based on configurations done via Global Customer Support. This impacts the deletion of both internal employee and external applicant applications. Global Customer Support uses the Location OU to manage different durations of time.

Note: To enable instant application data deletion and profile anonymization, contact Global Customer Support.

Data Deletion of Internal User Profiles

Internal Users are hired employees whose candidate records have transformed into a user record. Clients can configure the period after which user profile data is anonymized and their application information is deleted (time-based deletion) through the Legal Entity OU.

In the data deletion process for User Profiles, all application information is deleted while their name, email, and contact information is anonymized in the database. The scheme for core user data is based on the configuration defined for the user’s Legal Entity OU. A client can also request a one-off deletion of data for specific users (ad-hoc deletion). Data deletion is permanent and cannot be reversed.

An Internal User’s Data Deletion clock starts ticking once their status is changed to an inactive status (they are fired, quit, or request to be removed from the system). In this instance, all application information is deleted too.

Impacted Data

When either the application data deletion or user based data deletion event is triggered, all data for the user’s application is permanently deleted and will no longer be recoverable in the database. The following data will be deleted:

* Comments
* Ratings
* History / Audits
* Interviews
* Offer Letters
* Reviewers
* Selection Responses
* Realistic Job Preview
* Selection Assessment
* Skills Test
* Workflow Responses
* Competency Assessment Task
* Disclaimer
* EEO Question
* Training
* Custom Integrations
* Pre-Screening Responses
* Emails
* New Forms
* External Assessments
* Background Checks
* Attachments
* Flags
* Referrals / Costs
* Applicant Resume

When user based data deletion occurs, the above data points are deleted for ALL requisitions. In the case of only requisition data deletion occurs, the above data for only that specific requisition is deleted.

Users can request that their data be anonymized as a result of leaving the Legal Entity. Once the user leaves the Legal Entity, then their data is anonymized and the data cannot be recovered in its previously visible state.

This impacts the following areas of the system:

* Manage Applicants - Applicant profile data will be anonymized
* Recruiting Dashboard - Applies to the following:
	+ View Snapshot > Submission Details / "Name" column in All Submissions subsection (only when user leaves the Legal Entity)
	+ View Snapshot > Cost Details / "Applicant Name" column in Cost Details (only when user leaves the Legal Entity)
	+ View Snapshot > Cost Details / "Modified by" column in Cost Details (only when user leaves the Legal Entity)
	+ Recent Referrals / "Referred by" column
	+ Recent Referrals / "Name and Contact" column (only when user leaves the entity)
* Search Candidates - Applies to Saved Searches
* Review Applicants - Applies to Review Applicants / "Owner(s)" column
* Recruiting Manager Dashboard - Applies to the following:
	+ Recruiter Snapshot / "Recruiter name"
	+ Recruiter Snapshot / Recruiter name in Time to Hire drop-down
* Candidate Search Query - Applies to Saved Searches / "Created by"
* User Resume (not applicant resume)

See Also

* [**Ad Hoc Anonymization**](#_Ref-1139492740)

GDPR - Ad Hoc Anonymization

You can request to have applicant data anonymized on an ad hoc basis outside of the specified compliance settings timeframe and without forcing a candidate to log in to their profile to anonymize their own data.

This option is available in addition to the ability to enable anonymization in Compliance Enablement Preferences, a feature that lets you configure whether applicants can request anonymization and also allow the system to anonymize applicant data after a period of inactivity by the applicant.

Request Anonymization

To request ad hoc anonymization, submit a work order to Global Customer Support. Once the work order has been completed, the applicant will be anonymized, regardless of their period of inactivity.

If an applicant requests to be anonymized, and the applicant is still in an active status for an open requisition, the applicant will stay in their current status but no one will be able to interact with their profile after the anonymization takes place.

Note: To enable instant application data deletion and profile anonymization, contact Global Customer Support.

Use Case

1. Sarah has applied for a position at ACME, a European company based in Italy. Sarah would like her application anonymized for data privacy reasons, even though she applied a day ago. Her status is still active and is tied to an open requisition. Sarah does not want to log in to her profile to request the anonymization of her data. Instead, she emails ACME and requests that her email be anonymized.
2. Francis is an administrator at ACME. Francis creates a Global Customer Support work order to have Sarah's profile information anonymized.
3. When Francis views the active requisition, Sarah is no longer there. Instead, Sarah’s data has been anonymized, and Francis cannot access Sarah’s profile.

See Also

* [**Anonymization by User**](#_Ref-1989047182)