CommunityWFM

Data Privacy and GDPR

Webinar handout
Version: March 21, 2024

3400 Waterview Parkway, Suite 325
Richardson, Texas 75080

phone 877-668-6870
web CommunityWFM.com

Table of Contents

About this Document

This document accompanies the CommunityWFM College webinar *Data Privacy and GDPR*. It includes additional details and step-by-step instructions for completing the tasks discussed during the webinar.

A Brief Introduction to Data Protection Regulations

In recent years, many legislative bodies have created statutes governing the use and distribution of personal data for users of a web site or application. The original requirements emerged in the General Data Protection Regulation (GDPR) passed by the European Union in 2018, but more recently other countries as well as individual states within the U.S. have adopted the fundamental tenets of the legislation. As of December 2023, no federal data privacy statute exists in U.S. federal law, but several states (including California, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Oregon, Montana, Texas, Delaware, and Virginia) have adopted data protection laws similar to the GDPR.

The purpose of this legislation is to ensure that users of online services are aware of and consent to the use of their personal data and imposes requirements for storage and transmission of personal data to and from the online service.

Who are Data Subjects?

Generically, a "data subject" is any user of an online service (website or web application) that collects or processes personally identifiable information (PII). PII includes any information that can identify a platform user as an individual person and includes (but is not limited to) data points such as:

- First and last name
- Dates related to the person like birthdate or hire date
- Credit information
- Contact information (phone numbers, addresses, email addresses, etc.)
- Photos
- Usage data (i.e., activity history in a web application)

Data subject rights may vary between different data protection laws, but generally the list of data subject rights includes:

- The right to be informed about what kind of personal information an organization has about an individual. This right is commonly addressed through online Privacy Policies.
- The right to access personal information. This right is commonly addressed by creating an export of personal data.
- The right to rectification. This means that data subjects can challenge the accuracy of their personal information and ask an organization to update or correct personal information.
- The right to deletion. This is the right that has the most exemptions and exceptions, which means there are several reasons clients and/or CommunityWFM may choose or be required to deny these requests. Just because an individual asks for their personal information to be deleted does not mean that it must be deleted.
- The right to object to direct marketing and automated decision making.
- The right to restriction. This right is a temporary option if there is a dispute about the accuracy of personal information or the legality of using the personal information. If an organization no longer needs the personal information but the data subject needs the organization to keep the personal data without using the data for any other purpose, or the organization is considering whether to grant an objection request, so the organization restricts processing until the decision is made.
- The right to data portability. This right is similar to the right to access except this right is about data subjects being able to get their personal data from one organization in a common, machine-readable format so that the data subject can give that information to another organization for input into the second organization's systems.

Under the GDPR and other data protection laws, data subjects may exercise their rights by submitting a "Data Subject Access Request" (DSAR) to the online provider. The GDPR defines a 30-day time window for fulfilling the request. Other data protection laws may have shorter or longer timeframes to respond to data subject requests.

Fulfilling DSARs in CommunityWFM

CommunityWFM is responsible for helping organizations respond to data subject requests but is not able to fulfill those requests.

CommunityWFM supports direct fulfillment of the DSARs within the application by a designated "data privacy advocate." Any DSAR that requires administrative intervention will be fulfilled by the advocate, subject to the timeliness requirements of the regulations.

CommunityWFM personnel are not able to:

- Tell an organization if PII should be deleted.
- Tell an organization if PII should be modified.
- Tell an organization if PII should be restricted.
- Assess the validity of a DSAR.

Again, the role of CommunityWFM personnel is simply to guide an organization through the application's interface after deciding how to proceed with the DSAR.

CommunityWFM supports fulfillment of a DSAR by two means:

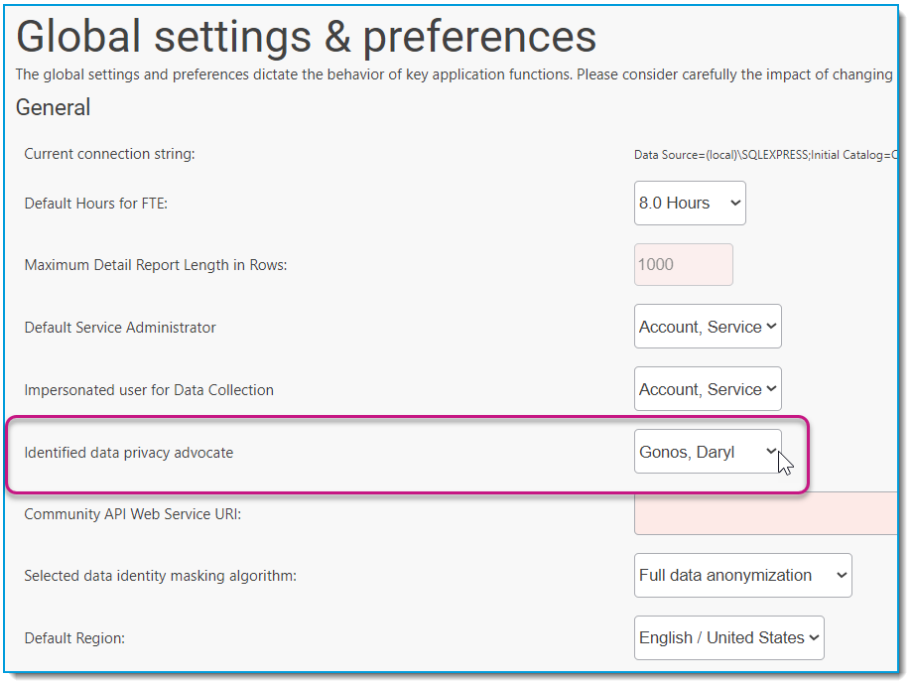
- End-users may exercise a right in a purely self-service manner; that is, no administrative intervention is required.
- End-users may exercise a right that requires administrative intervention.

In either case, the DSAR is logged in an audit table and available for review. For any DSAR that requires administrative intervention, the application will notify the data privacy advocate using the established notification channels (such as internal memos, external email gateway, SMS/text messaging, Teams, Slack, Webex, or mobile devices). The responsibility for fulfilling the DSAR rests solely with the advocate (or delegated to another administrator).

Designating a data privacy advocate

CommunityWFM 5.1 supports the ability to designate an administrator-level user as the data privacy advocate. In the ***Global settings & preferences***, select the designated person to respond to and fulfill requests regarding DSARs.

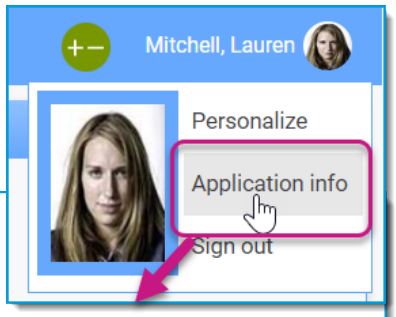
The default for this field is the initial service account and should be changed to a designated administrator.



The Data Subject Rights Policy in CommunityWFM

CommunityWFM 5.1 includes the application's data subject rights policy as an embedded part of the user interface. Any user of CommunityWFM may access the policy by navigating to the personal menu (under the username) and selecting *Application info*.

A new "Data Subject Rights" section includes a link to the policy and a link to view previous requests.



The application allows a user to exercise their data subject rights directly from the policy page (*Click here to review the data subject rights policy*). For more information, see Additional Resources.

The right to be informed

*What personal information will Your Employer **always** collect?*

- Your first name.
- Your last name.
- Your company employee ID.
- Your company email address.
- Your primary work location.

*What personal information will Your Employer **sometimes** collect?*

- Information related to time off requests, including dates, request type, and comments.
- Information related to accrued time off balances.
- Information related to certain corrective actions or restricted access plans, including supporting documents and comments.

What personal information can you elect to opt in or out of (optional personal information)?

- Your photo used within the application.
- Your personal telephone number(s) used for text message notifications.
- Your personal email address(es) used for email notifications.
- Your mobile device information, including operating system, device ID, device model, and manufacturer if you are licensed for and elect to use the Community Everywhere mobile application for iOS and Android devices.

How does CommunityWFM use any of the above information listed above?

- Normal application and business functions, including scheduling, reporting, and notifying users of important application-related events.
- Notifications of important system events may be shared with 3rd party gateway providers (Teams, Slack, Twilio) and may include first and last name, time off approval status, and restricted access information.

Additional Information

This right provides the necessary transparency between CommunityWFM and end-users of the application by defining what data is collected and how it is used. The application

requires the information above to perform the core functions related to scheduling and reporting for users.

The right to access

You have the right to access the information that has been collected for you as an application user. If you wish to access your personal data, please click the link below and provide the relevant information.

Click here to access your personal information. ***(For illustration only. Link is active on the webpage).***

Additional Information

The right to access allows data subjects to review all the personal data that the online service has collected about them. In CommunityWFM, this includes the above stated information, in addition to the skill assignments and custom fields defined at the time of installation for users. Note that this is a self-service DSAR. The result is a page containing read-only values for all agent properties, similar to the current "Profile" page accessible to agents.

The right to rectification

You have the right to request a correction to any inaccurate data collected by CommunityWFM as entered by your employer. If you wish to request a change to your personal data, please click the link below. You must provide exact details regarding the data inaccuracy as well as the corrected values. Note that your request should be satisfied within 30 days after you submit your request.

Click here to rectify your personal information. ***(For illustration only. Link is active on the webpage).***

Additional Information

The right to rectification allows users to submit requests for changes to their personal data, either because the data changed or because it is inaccurate. Exercising this right requires that the user provide specific descriptions of the inaccurate values as well as the correct values. Note that this request requires intervention by the data privacy advocate in order to fulfill the request.

The right to erasure

Your employer does not guarantee the right of your data to be deleted at any time. The application retains your required personal information for historical reporting and budgeting purposes.

However, you may elect to have your data anonymized once you are no longer a user of the application. In addition, you may elect, at any time, to have any optional personal information removed from the application's database. Note that your request should be satisfied within 30 days after you submit your request.

Please refer to the following options related to data erasure.

Click here to indicate that you would like your personal data anonymized upon cessation of employment. ***(For illustration only. Link is active on the webpage).***

Click here to remove all optional personal information. ***(For illustration only. Link is active on the webpage).***

Additional Information

The right to erasure conflicts with the need for historical retention of schedule and adherence data for aggregate reporting purposes, the ability to provide our services, and sometimes with other laws. Therefore, neither clients nor CommunityWFM support full erasure of any user's data as a result of a DSAR.

However, CommunityWFM will support two options to satisfy the right to erasure. Briefly, anonymizing a user's data sufficiently obfuscates the user's data in a way that forever prevents anyone from identifying the actual person represented by that user. See ***Additional details on CommunityWFM anonymization algorithms.*** *Note that data anonymization requires intervention from the data privacy advocate.*

Removing all personal data will immediately remove any of the optional data points described under the Right to be informed rule, including user photos, any device information (mobile device, phone numbers, etc.) and any personal email addresses.

Note that removing all optional personal information does ***not*** *require intervention from the data privacy advocate.*

The right to restrict automatic data processing

Your employer does not guarantee the right to restrict automatic data processing. The fundamental purpose of the application is to automate schedule generation as well as manage (approve or deny) time off requests. In the interest of efficiency, the application implements automated processes for achieving these results. Therefore, application users are not eligible for restricted data processing activities.

The right to data portability

You have the right to retrieve in a machine-readable format the information that your employer has collected for you as an application user. The application allows you to export your personal data into a comma-separated values (CSV) file format. However, the data export restricts access to confidential or proprietary company information.

Click here to request your personal information. ***(For illustration only. Link is active on the webpage).***

Additional Information

The right to data portability theoretically allows a user's data to be moved from one platform to another. While that is not a practical reality for the type of data collected for any user, the application supports the right to retrieve the personal information in a CSV file. The application exports all information found in the "Right to be informed" section to a CSV file using the system assigned agent id as a file name. Note that a warning message will appear alerting the user that, once the data is exported, CommunityWFM is no longer responsible for protecting it.

Note that exporting the user's personal information requires intervention from the data privacy advocate. This is to ensure that the exported file does not contain confidential information.

The right to object under certain conditions

You have the right to object to the processing of personal data within CommunityWFM by your employer. However, in order to function the application must process the required personal information described above. Note that **Your employer** does not distribute any personal data to direct marketing organizations.

The right to restrict processing

Your employer does not explicitly guarantee the right to restrict processing. If you feel that you are entitled to request the restriction of data processing, please contact your data privacy advocate. Your system's data privacy advocate is **WFMSG, Admin A**.

Additional Information

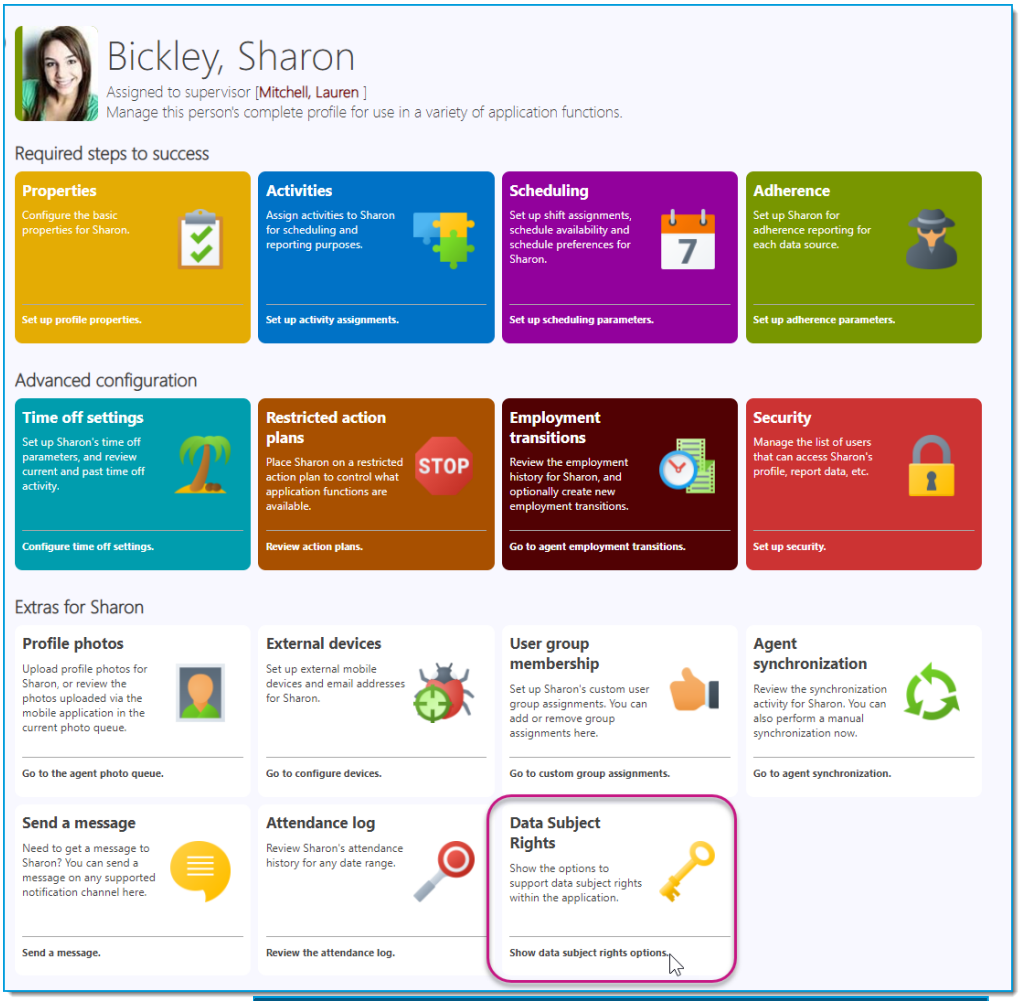
The right to restrict processing is a "manual" process within the application, and thus the data subject rights policy points users to the data privacy advocate.

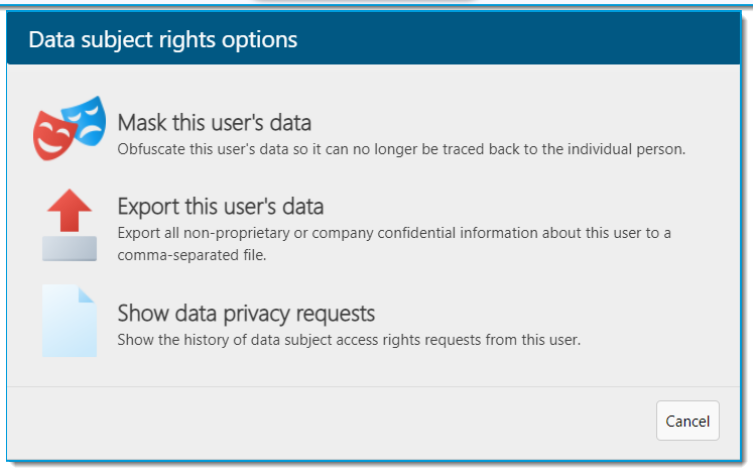
Additions to Personal Information Gathered or Collected

Your Employer may, on occasion, collect or gather additional personal information. If this occurs, your data privacy advocate will inform you of the new personal information being collected and the justification for doing so. If you have any questions about this policy, please see your data privacy advocate. Your system's data privacy advocate is **WFMSG, Admin A**.

User profile enhancements

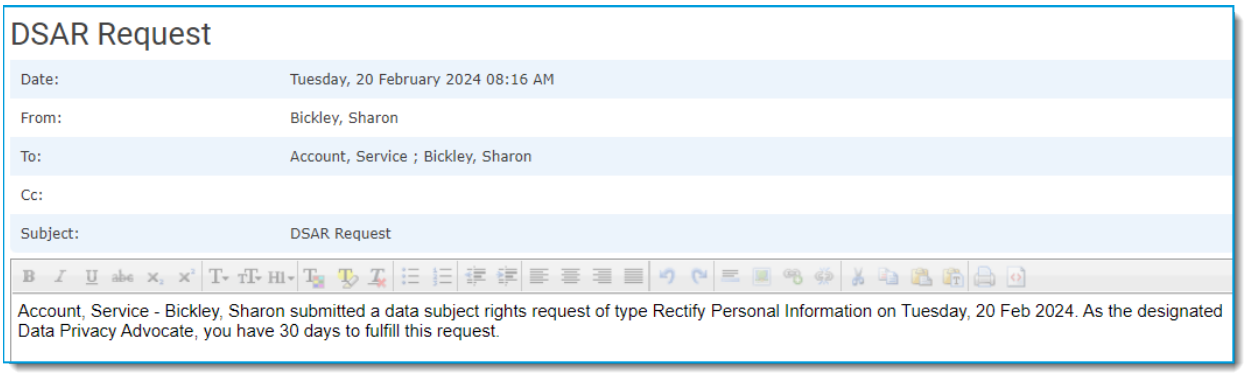
Community 5.1 offers features to facilitate compliance with GDPR by making data subject rights a first-tier element of the user profile. The feature tile *Data Subject Rights* serves as a launch point for additional features related to data subject rights.





Responding to a request

When a request is made, the data privacy advocate will receive a notification of the type of request.



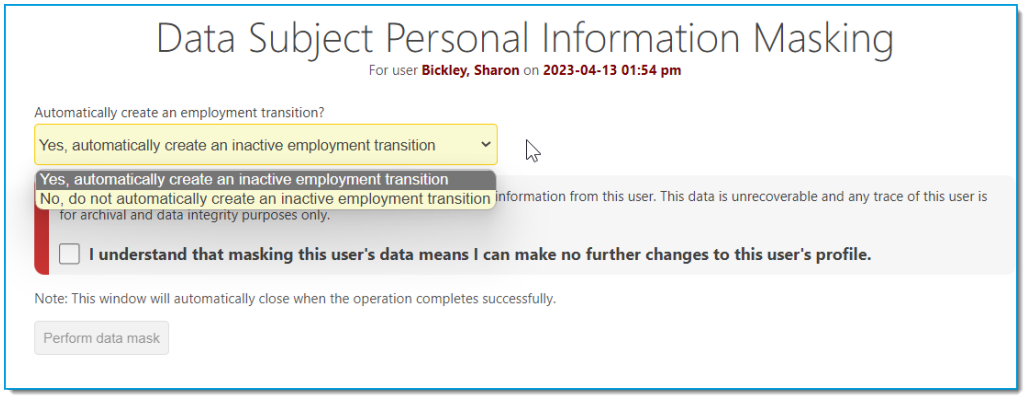
To fulfill the request, the advocate should navigate to the person's personal profile, select ***Show data subject rights options,*** then select from the options.

Mask this user's data

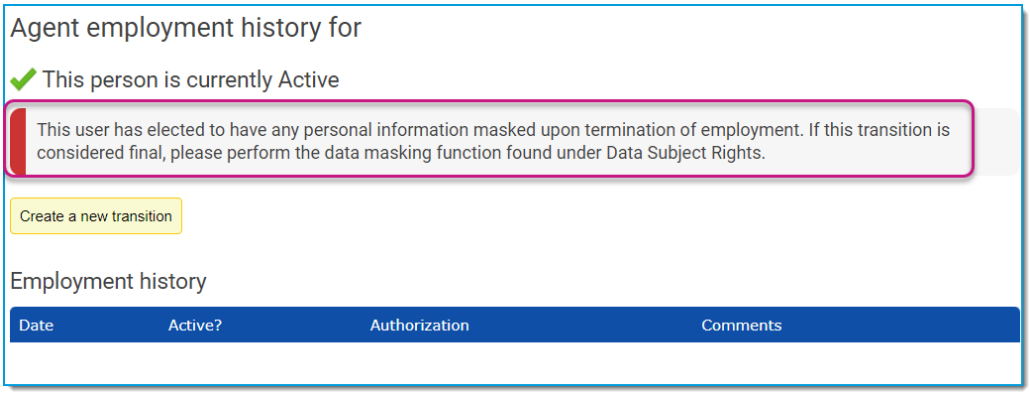
See Data Masking Algorithms for details on the various data masking algorithms available in the application.

Masking user data with full anonymization is permanent and cannot be reversed

This option allows the data privacy advocate to scrub or mask the user's data to prevent identification, subject to the rules of the selected masking algorithm in the Global settings & preferences.



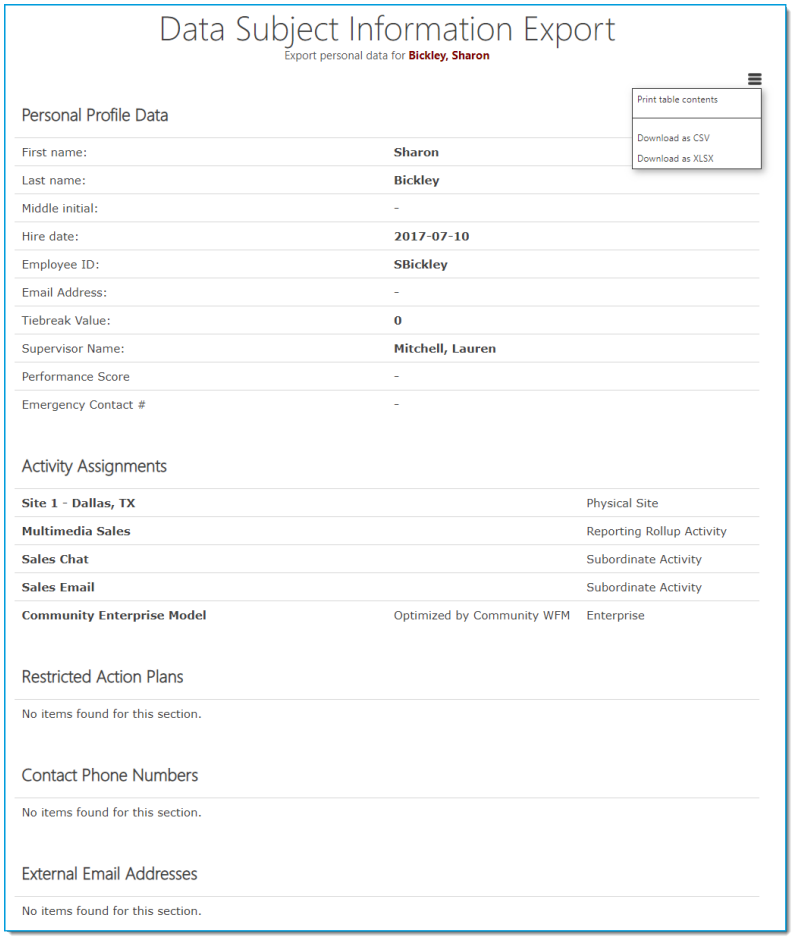
If an agent requests that their data be masked at the end of employment, the request is automatically marked as complete, and when creating an employment transition, you will see a message regarding the request.



Export this user's data

This option exists to facilitate a user's right to data portability and requires that the privacy advocate export the information to a file and provide it to the requesting user within 30 days of the request. (**Note: the 30-day response time is dictated by the applicable privacy laws and is a configurable parameter within CommunityWFM.** To change the response interval, a technical services representative must access the application database.)

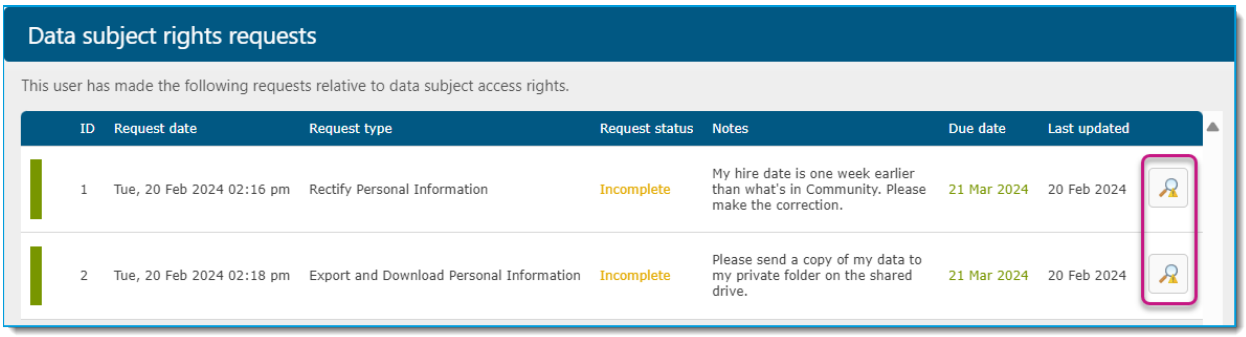
There are two options for exporting – "Download as CSV" and "Download as XLSX." The CSV download creates a simple text file with no formatting while the XLSX download creates a formatted Excel file.



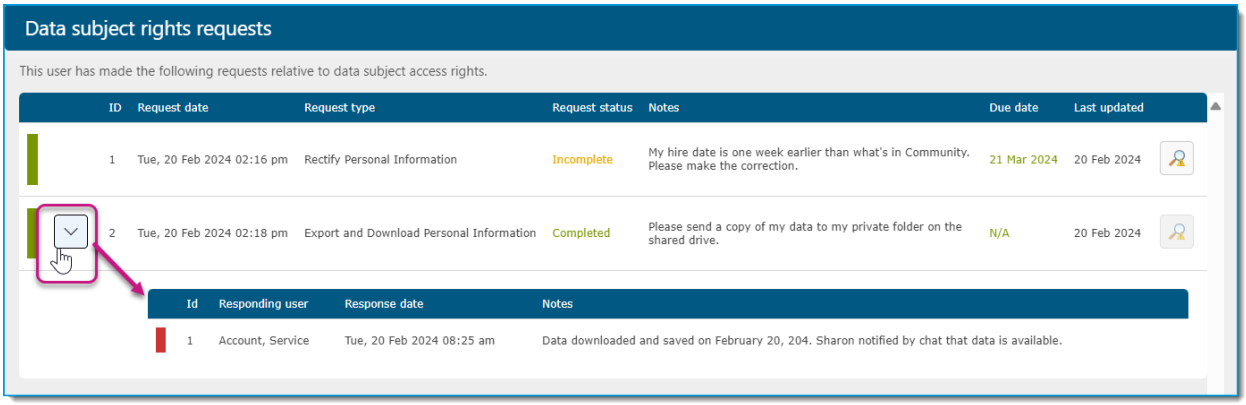
Show data privacy requests

This option exists to allow the privacy advocate to review DSARs for a specific user. CommunityWFM will automatically create data privacy requests when a user clicks any link or submits any request while exercising any of the data subject rights described earlier. This includes exercising those rights that do not require intervention from the data privacy advocate.

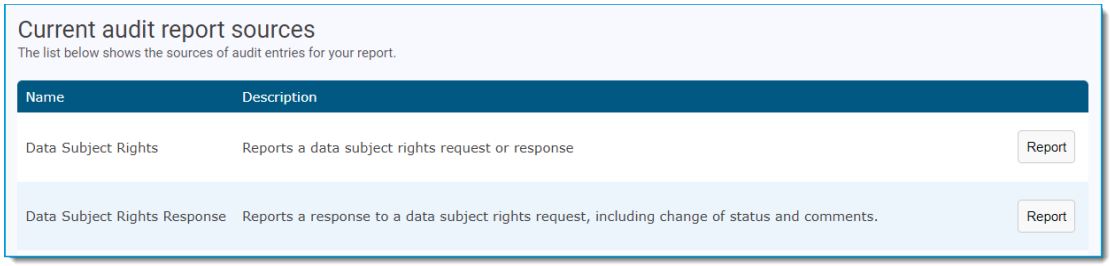
Click on the magnifying glass to complete the request or mark it as invalid.



Completed requests include a carat to view the response.

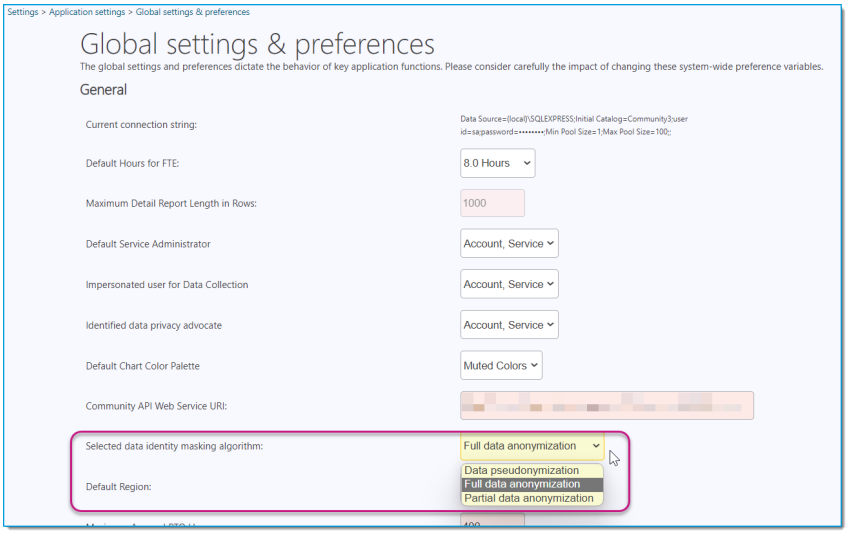


To view all data privacy requests and responses, go to Report > Administrative & utility > Change audit log and select the Security tile. There are two report options.



Data Masking Algorithms

CommunityWFM supports three data masking algorithms. Note that the data masking algorithm is a global setting and will apply to all data masking operations for all users.



Full Anonymization

This algorithm scrubs the personal data for any information that may serve as an identifier to a user.

Data Property	Scrubbing Method
First Name	Random 10 characters
Last Name	Random 10 characters
Middle Initial	Blank / NULL value
Hire Date	01 Jan 1900
Supervisor Assignment	No assignment – NULL value
Tiebreak Value	0
Email Address	Blank or NULL value
Title	Blank or NULL value
Time Zone	NULL value
Custom Profile Properties	**All** returned to blank or NULL value

Other properties

Note that activity assignments must be retained to satisfy reporting requirements. However, the application permanently deletes the following additional data points with full anonymization:

- Schedule preferences
- Schedule availability
- User group assignments
- Pending time off requests
- Device information (mobile numbers or mobile device IDs)
- External email addresses
- Restricted action plan details
- Schedule transactions (swaps, takeaways, giveaway, etc.)
- Agent synchronization logs, membership (as a source or direct target)
- PTO calendar participation
- ASAP participation
- Existing notifications, messages, or pop-up reminders
- Connection to data source (optional – this may be configured to use an anonymized login for future adherence reporting)
- Schedule template assignments
- "To Do" items list

Additional notes

Full anonymization will ***prevent any further edits to the user account (profile)*** to guarantee that the user can no longer have access to the system and no user (not even a super user or administrator) can "reactivate" an anonymized user.

The administrator performing the data masking function has the option to automatically create an employment transition to inactive to "deactivate" the user.

There is an audit trail that records who performed the masking and when. This is the only place in the system that retains the agent's name.

Partial Anonymization

This algorithm provides a similar degree of obfuscation to the full anonymization algorithm but leaves the user profile in an editable state.

Pseudonymization

This algorithm scrubs the data but in a way that reduces, but does not eliminate, the ability to link the data back to a user. This algorithm leaves the user profile in an editable state.

The properties and method of scrubbing the data are as follows:

Data Property	Scrubbing Method
First Name	The user's system assigned User ID
Last Name	The user's system assigned User ID
Middle Initial	Blank or NULL value
Hire Date	Does not change
Supervisor Assignment	Does not change
Tiebreak Value	Does not change
Email Address	The user's system assigned User ID concatenated with the existing email domain address
Title	Blank or NULL value
Time Zone	Does not change
Custom Profile Properties	All returned to blank or NULL value

Other properties

Note that activity assignments must be retained to satisfy reporting requirements. However, the application permanently deletes the following additional data points as a result of pseudonymization:

- User group assignments
- Pending time off requests
- Device information (mobile numbers or mobile device IDs)
- External email addresses
- Restricted action plan details
- Schedule transactions (swaps, takeaways, giveaway, etc.)
- Agent synchronization logs, membership (as a source or direct target)
- PTO calendar participation
- ASAP participation
- Existing notifications, messages, and pop-up reminders

Additional notes

Pseudonymization will leave the user profile in an editable state, similar to partial anonymization, so that, if desired, a change to the profile is available.

Additional Resources

If you want to read the complete GDPR text:

Complete GDPR Text

If you want to read the complete GDPR compliance guide:

Complete Guide to GDPR Compliance

If you want to read specifically about data subject rights:

GDPR Rights of the Data Subject