



# MindaClient GDPR User Guide

# Table of Contents

<b>Permissions and Consent .....</b>	<b>3</b>
<b>Opting Out.....</b>	<b>5</b>
<b>GDPR Administration .....</b>	<b>6</b>
<b>Anonymising Clients.....</b>	<b>7</b>
<b>Deleting Clients .....</b>	<b>9</b>
<b>Data Cleansing.....</b>	<b>10</b>
<b>Restricting Permission for users.....</b>	<b>12</b>
<b>Password Security .....</b>	<b>13</b>
<b>Audit Trail.....</b>	<b>14</b>
<b>Requests for Copy of data .....</b>	<b>15</b>
<b>Managing SARS Requests.....</b>	<b>15</b>

## Permissions and Consent

There are a number of permissions that you should get in order to process the data on behalf of a person. We have updated our permissions section in the client and the contact profile.

When you move your mouse over the help question mark icon you will see an explanation of each permission. These are explained in more detail below.

The screenshot shows a 'Permissions' section with a 'hide' button. The permissions listed are:

- Date Data Checked:  [calendar icon] \* [help icon]
- Informed of Right to Object to Processing:  [help icon]
- Object to Processing:  [help icon]
- Basis for Processing:  \* [help icon]
- Consent to Process Data:  [help icon]
- Date of Consent:  [calendar icon] \* [help icon]
- Receive SMS:  [help icon]
- Receive Emails:  [help icon]
- Receive Letters:  [help icon]
- Permission For Photo:  [help icon]

A tooltip for the 'Date Data Checked' field reads: "Date you last checked the Accuracy of the data."

### Client Permissions

PERMISSION	EXPLANATION
Date Data checked	This is the date that you last checked the Accuracy of the data. This would be in accordance with your own policy. Do you check every six months. Do you check every year. Do you check each time a client rings in. There is the facility in the Client reporting to filter a list of all the clients whose date last checked was over a year ago for example.
Informed of Right to Object to Processing	You have informed this person of their right to Object to have their data processed under GDPR.
Object to Processing	If ticked this would indicate that the person has objected to you processing their data. If this box is ticked then the Tick boxes - Receive SME, Receive Email, Print Labels will be automatically blanked out. If the person doesn't want their data processed then they do not wish to receive Texts, Emails or a label.

Basis for Processing	<p>This is probably one of the most important items to record under GDPR and it is the basis which you are relying upon to process their data.</p> <p>The different bases are listed below so it should be one of these.</p> <ol style="list-style-type: none"> <li>1. Compliance with legal obligation</li> <li>2. Contract with client</li> <li>3. Vital interests</li> <li>4. Public interest</li> <li>5. Legitimate interests</li> <li>6. Consent received</li> </ol>
Consent to Process Data	The person has consented to you processing their data. Note this only applies if the above Basis for Processing is Consent received.
Date of Consent	The date the person has provided consent. This field will be updated every time you email or text the client through MindaClient with an option to opt out. Note this only applies if the above Basis for Processing is Consent received.
Receive SMS	If this is ticked, then the person can receive Texts
Receive Email	If this is ticked, then the person can receive Emails
Receive Letter	If this is ticked, then a label can be printed for the person.
Permission for Photo	This person has given consent to let you use their photograph

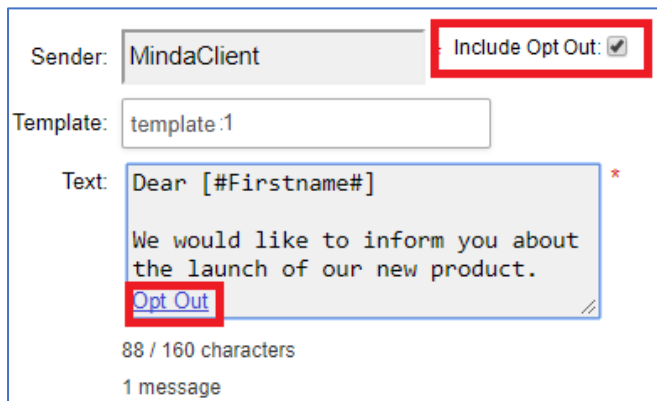
## Bulk Updating permissions

You can bulk update the above fields in the Edit Records section in Client Reporting. For example you might wish to filter all your current clients and update them to say that the basis for processing is the fact you have a contract with them.

You do this as follows

1. Click on Reporting & Client Reporting
2. Filter your clients
3. Click on Edit Records
4. Select Receive SMS = Yes in the dropdown list at the top of the list if you want to update selected clients to Yes for Receive SMS.
5. Tick to select your clients
6. Click Update and following the instructions.

## Opting Out



The screenshot shows the MindaClient communication editor interface. It includes a 'Sender' field with 'MindaClient', a 'Template' field with 'template:1', and a 'Text' field containing a message. The 'Include Opt Out' checkbox is checked and highlighted with a red box. The 'Opt Out' link in the text is also highlighted with a red box. The text field shows '88 / 160 characters' and '1 message'.

MindaClient now has a simple tickbox that is available for bulk communication to clients.

This is built into the Email communication and the Text communication.

You just tick the “Include Opt Out” tickbox and the recipient will have the option to opt out.

### Opt out option for texts

Communications such as newsletters should always include the option to opt out.

If the recipient opts out from an email communication then their Receive Email tickbox in MindaClient will be unticked automatically.

If the recipient opts out from an SMS communication then their Receive SMS tickbox in MindaClient will be unticked automatically.

#### To set the opt out in communications

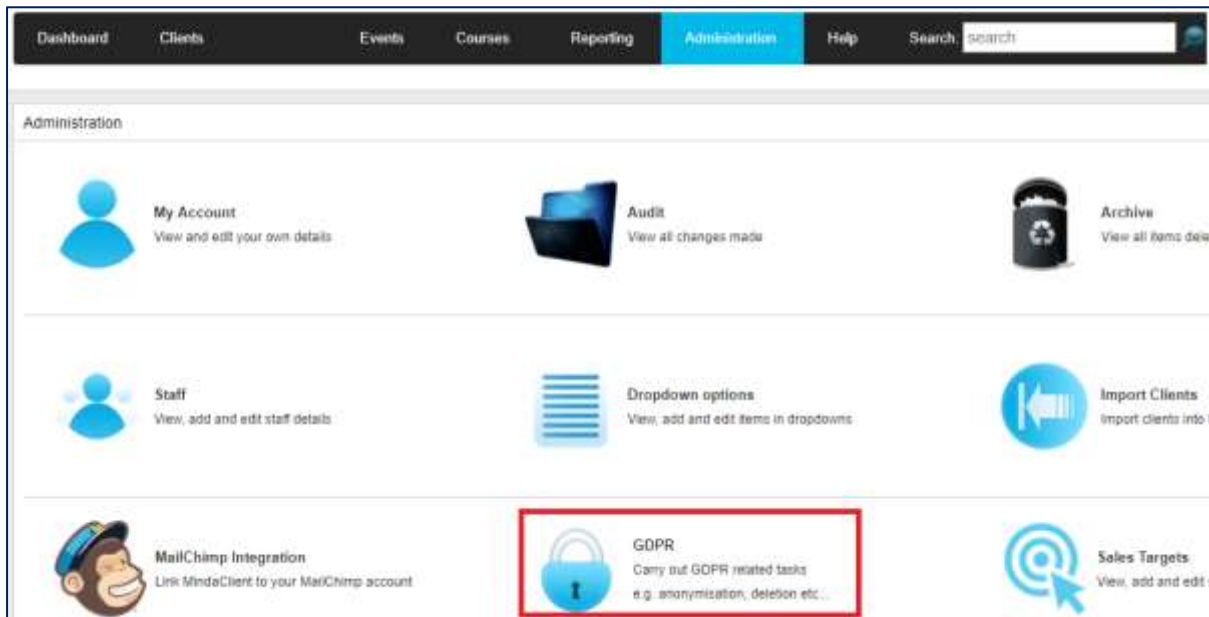
1. In the Client Reporting screen you filter your clients and click Send Email or Send Text
2. On the send screen you tick the “Include Opt Out” tickbox
3. You send the email or text as normal.

If a client has opted in and their Date of Consent has been filled in in MindaClient then this date will be automatically updated in MindaClient when you send them a bulk communication with the option the opt out.

That is because the Consent is meant to be renewed under GDPR and if you are communicating with your clients who have already opted in and giving them the option of opting out then that is deemed to be an update of their consent.

# GDPR Administration

Under our new GDPR administration we have provided the facility to Anonymise data subjects if you need to and to delete clients as part of only retaining data as long as you need it. You can click on the new GDPR link in the Administration section.



## GDPR Administration

The GDPR Admin link opens up the following three options which will let you Anonymise Data, Set which additional fields you wish anonymised and delete Clients.



## GDPR Administration options

## Anonymising Clients

You can anonymise Clients and Contacts in bulk. There are checks and confirmations in place to ensure that data is never anonymised without user express confirmation.

Anonymising of data is permanent and cannot be undone.

Anonymising of a client or contact will involve removing the following from their record.

- First name
- Surname
- Address
- Phone number
- Mobile
- Email Address

Once you click on the Anonymise link you will see the Anonymise Screen.

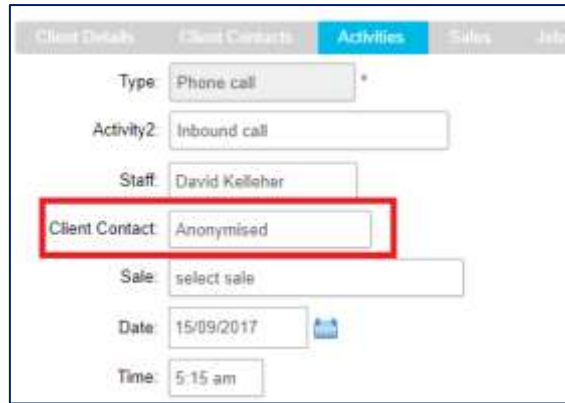


### Anonymise Contact Screen

The Steps to Anonymise a persons' details are as follows

1. Click on GDPR Administration and Anonymise link
2. Enter your search criteria on the left hand side and click Search.
3. Review the search results on the right hand side and tick the person that you definitely wish to Anonymise.
4. Click the Anonymise button on top of the screen and follow the instructions doubly confirming that you wish to proceed to anonymise the person.

Activities such as sales, meetings, jobs that have previously been recorded with this contact will still remain in MindaClient but the contact that they have been linked to will simply display "Anonymised" The name of the company or organisation which is not personal information will remain.

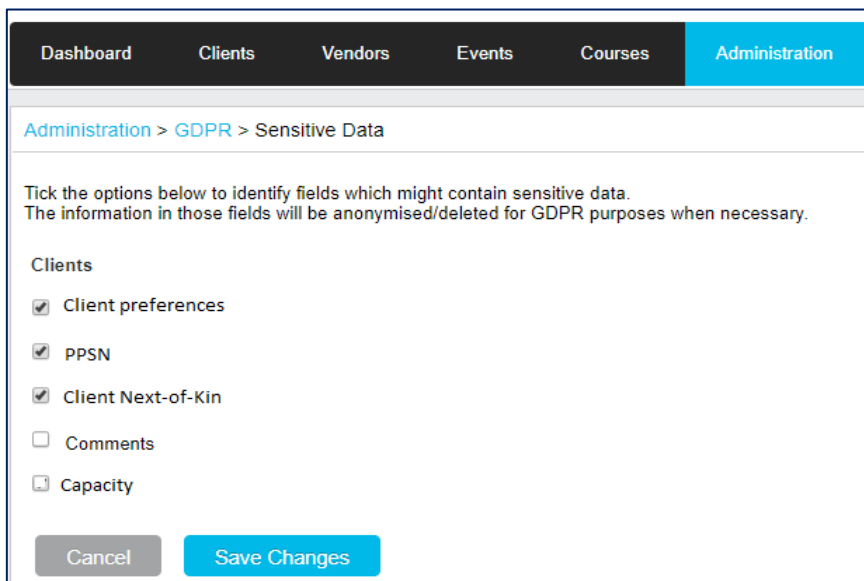


**Activity with contact who is now anonymised**

Extra client text fields can be set up for clients in MindaClient. Sometimes these fields will also contain personal information that you may wish to anonymise as well as the personal information outlined above.

Your administrator can set which fields that you want to be automatically anonymised for clients when you go through the anonymising function.

In the example below the client fields “Client Preferences, PPSN & Client Next-of-Kin would all be anonymised if the options below were set.



**Anonymising Sensitive data fields**

Here are the instructions to set extra text fields to be anonymised when you are anonymising clients.

1. In the Administration section click on the GDPR link and click on Admin
2. Tick the text fields that you want to be automatically anonymised when you anonymise a client.
3. Click the Save Changes button



## Deleting Clients

Once you have decided what your policy is you can filter your clients in MindaClient and proceed to delete them based on your own criteria.

This bulk delete facility is only available at Administration level. There are multiple checks built in to ensure that data is never deleted in error.

In the GDPR Admin section you click on the Delete Clients link.

You can filter by client fields or by date last updated.

The screenshot shows the 'Delete Clients' interface in MindaClient. The navigation bar includes 'Dashboard', 'Clients', 'Events', 'Reporting', 'Administration', and 'Help'. The breadcrumb trail is 'Administration > GDPR Menu > Delete Clients'. There are two main filter sections: 'Filter by Client' and 'Filter by Activity'. The 'Filter by Client' section includes dropdowns for Client Type, Group, County, Staff, and Country, and date pickers for D.O.B. Between and First Contact Between. The 'Sector' dropdown is highlighted with a red box and set to 'Engineering'. The 'Filter by Activity' section is also highlighted with a red box and includes a list of activities (Activities, Client Contacts, Sales, Jobs, Documents) and a 'Date' field set to '01/04/2016'. A 'Bulk Delete Report' button is located on the right side of the page.

**Bulk delete screen**

The above filter would return all the Engineering companies that you haven't updated since 01/04/2016.

Once you click on the Bulk Delete link then the clients that meet your criteria will be displayed as shown below.

You then have to tick the client or clients that you want to delete and click the delete button.

The screenshot shows the 'Delete Clients' interface with a list of clients. The client 'Brian McEvoy' is selected. A 'Delete' button is highlighted with a red box. A 'Confirm Delete' dialog is open, asking for confirmation to delete the selected record. The dialog text reads: 'You are about to delete 1 selected record. Are you sure you wish to continue?'. The dialog has 'Cancel' and 'Continue' buttons. Below the list, there is a table with columns: Type, Client No, Organisation Name, Firstname, Surname, Addressline1, Addressline2, Addressline3, and Addressline4. The data row shows: Individual, 1048267, MindaClient, Brian, McEvoy, PM2764876, 1A McKinney Road.

**Delete Confirmation**

You will be asked to confirm the deletion and because the deletion cannot be undone you have to type in the word delete as shown below.



**Typing delete to confirm deletion**

Once you go through the above procedure to delete a client then that data is instantly and completed delete and can NOT be retrieved.

To provide a level of transparency the audit does record who has carried out a bulk deletion, when it was carried out and how many clients were deleted.

Deletion of data is a final step and should be carried out in accordance with your own retention policy under GDPR.

Summary of the steps to delete clients in bulk.

1. In the Administration section click on the GDPR link and click on Delete Clients
2. Select the group of clients based on client profile or date since updated
3. Click Bulk Delete Report
4. Tick the clients you wish to delete, click Delete and follow the instructions

## Data Cleansing

MindaClient provides facilities to help you keep your data accurate and up to date.

### Bulk Updating

In MindaClient you can filter your clients and then carry out bulk updating on sections of your client base. Here are some examples of how this could be relevant to your company under GDPR.

- For existing clients, you could update your clients and contacts to remove permission to communicate by Text, Email or printing labels.
- You could filter a section of your clients and archive them at the end of the year.
- You could assign all clients from one sales person to another with staff turnover.

#### Instructions for Bulk Updating

1. Click on Reporting & Client Reporting
2. Filter your clients
3. Click on Edit Records
4. Select the value in the field in the dropdown list at the top of the list that you want to update.
5. Tick to select your clients
6. Click Update and following the instructions.

### Deduplicating data

MindaClient warns you if you are adding a client that is in already. However If you do come across any duplicated data you can combine the records using our Merge Client facility

Firstname	Surname	Address	Phone
Brian	McEvoy	1 High Street, Kilkenny	056 777777

#### Message you will see if you add a client that is already in your database

If you do come across two clients that should be combined into the one you can merge these two clients. Activities, Sales, meetings, Jobs and Client comments will all be combined in the new record.

To merge two or more clients you do the following.

1. Click on the Clients tab
2. Enter your Search criteria
3. Click on the Search to Merge button on the bottom right.
4. Beside the Search to Merge button there is a Help link that gives more detailed instructions on merging.

Search      Search to Merge Records ?

#### Merge Client Link

## Restricting Permission for users

MindaClient provides the facility where you can set access rights for users, ranging from full administration rights to all data, right down to read only or mobile only access rights.

You can also set a users permission so that they only see the clients linked to them. To do this you click the “View users clients only” tickbox for the staff member.

Access rights are important so that users only have access to the data that they are entitled to see.

The screenshot shows the 'Edit Staff Details' page in the MindaClient administration interface. The page is divided into two main sections: 'Details' and 'Permissions'. The 'Details' section includes fields for Title, First Name, Surname, Phone, Email, Password, Location, Active status, Administrator status, User Access (set to 'Manufacture and Sales'), Employee Hourly Rate, Show Prices In Job, Send Activity Report to, and Send Pipeline Report to. The 'Permissions' section contains a list of 20 checkboxes, each with a question mark icon, representing various access rights such as 'Merge Clients', 'View Clients', 'View Client Details', 'View Activities In Job', 'Show in Activities', 'View Reporting', 'View Diary', 'View Sales', 'Notification of New Sale Added', 'View Confidential Activities', 'View User Clients Only', 'View Bulk Editing', 'View Users Diary Only', 'Daily Summary Report', 'Daily Summary Activities Report', 'Weekly Summary Report', 'Show Company Charts On Dashboard', 'View MailClient Reporting', and 'Sales Targets'. At the bottom of the page are 'Cancel' and 'Save Changes' buttons.

**User Access permission screen**

To change the access rights for a user you do the following.

1. Click on Administration section
2. Click on Staff and click on the member of staff you wish to update.
3. Tick or untick the relevant tick boxes for the user and click save.

If you move your mouse over the question mark beside each item it explains what each permission does.

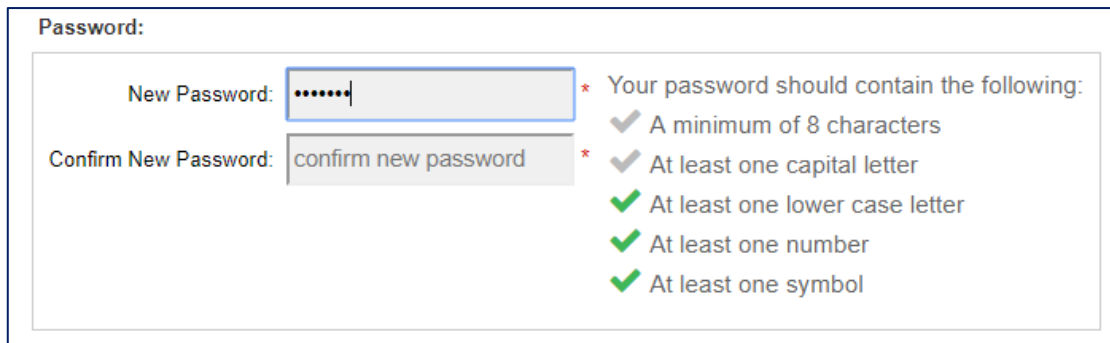
## Password Security

We have built in additional security around your password.

### Changing Passwords

In order to change your password you do the following

1. Click on “My Account” in the top right hand side of the screen.
2. Click on Edit my Account and Click on the Change Password link
3. Enter your new password. As you type in the password you will see the ticks appearing to confirm that a secure password has been entered.
4. Type your password in a second time to confirm it.
5. Click the Save Changes button at the bottom of the screen.



The screenshot shows a 'Password:' section with two input fields: 'New Password:' containing six dots and 'Confirm New Password:' containing the text 'confirm new password'. To the right of these fields is a list of validation rules, each preceded by a checkmark icon. The first rule, 'A minimum of 8 characters', has a grey checkmark. The other three rules, 'At least one capital letter', 'At least one lower case letter', and 'At least one number', each have a green checkmark. A fourth rule, 'At least one symbol', has a grey checkmark. The text 'Your password should contain the following:' is positioned above the first rule.

### Change Password facility

In addition to the above your password on our server is hashed. This means that in the unlikely event of anyone ever accessing the server they would not even see your password.

### Forcing change of Password

There is a new facility that you can set so that your users have to reset their password after a set period. You decide if this feature is to be turned on and you decide how often the users have to change their password.

When the time comes for users to change their password they will be able to login but after they login they will be forced to select a new password.

### Password Expiry Screen

To set up the forced change of passwords for your users you do the following.

1. Click on the Administration section and click on Settings
2. Click on Password Expiration as shown above and click on Change Policy
3. Select Yes in the Password Expiration Policy and enter the length of time in days that you want to set for users passwords to expire
4. Click Save Changes

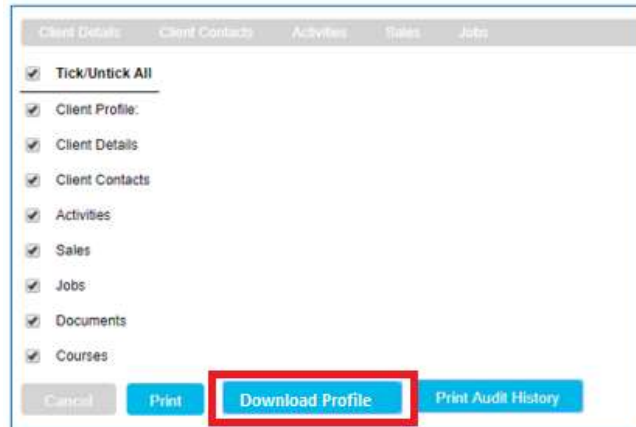
## Audit Trail

There is an audit trail running in MindaClient and this tracks all changes by users. It records

- The person who added the record
- The value before the change was made
- The person who made the change
- The date and time of the change
- The new value of the data
- It records when a user accessed MindaClient
- It records changes to dropdown lists

If you wish to view the full audit trail for a client, you do the following.

1. Search for the client and click into their record
2. Click on the Print Client Profile link on the left hand side
3. Tick or untick the types of records you want to check the audit for
4. Click the Print Audit History button



**Audit Trail and downloading personal data**

## Requests for Copy of data

A Data Subject or person is entitled to ask for a copy of the personal data you hold on them.

We have built a new download facility that will let you extract this information.

You can do this as follows.

1. Search for the client and click into their record
2. Click on the Print Client Profile link on the left hand side
3. Click the Download data (GDPR) button as shown above.
4. This will download the information to a CSV file. This could be saved to a memory stick and handed to the Data subject. Note that you should always encrypt a file if you are sending it by email.
5. You can click into a clients contact and download the contact data for GDPR also

## Managing SARS Requests

**Please contact us if you wish to have this feature set up in your MindaClient as this will involve updating your Activity dropdown lists.**

Under GDPR a person is entitled to make a number of requests to you as a data controller. These are referred to as Subject Access Requests or SARS.

- They can ask what information you hold on them
- They can ask you to correct data you hold on them
- They can request a digital copy of the information you hold on them
- They can request that you delete the data you hold on them
- They can request to know what is your data retention period

You are meant to deal with these requests as soon as possible and the maximum time limit is 30 days. If you do not comply with a Subject Access Request the person can make a complaint to the Data protection Commissioner.

More information about requests here <https://dataprotection.ie/documents/AccessGuidance.pdf>

MindaClient has developed a system that will allow you to process all requests from Data subjects.

The screenshot shows the 'Activities' form in MindaClient. The 'Type' field is set to 'GDPR'. The 'Activity Level 2' dropdown menu is open, showing options: 'select activity level 2', 'Request to Restrict Processing', 'Compliance Preparation', 'SARS Request Outstanding', 'SARS Request Completed', 'Request to Erase Outstanding', 'Request to Erase Processed', and 'Client Enquiry'. Other fields include 'Staff' (Brian Kelly), 'Client Contact' (Mary White), 'Date' (14/03/2018), 'Time' (9:10 am), 'Duration' (0 hours 30 minutes), and 'Comments'. There are checkboxes for 'Staff Reminder' and 'Outstanding', and buttons for 'Cancel' and 'Add Activity'.

When you receive a request you can record it in MindaClient for the relevant client.

You can record the following :

- The type of request
- The person who took the request
- The person who made the request
- The date of the request
- The time of the request
- How long you spent processing the request
- Any other comments

You can set reminders and follow ups to ensure all requests are processed.

You can report on all requests in the reporting section

#### Processing requests in MindaClient

Here are the instructions for dealing with a SARS request in MindaClient.

1. Search for the client and from the search results click on Add Activity
2. Select the Activity type as GDPR. (If this is not set up in your system you can contact MindaClient)
3. In the Level 2 Activity select SARS request
4. Enter the details of the request in the comments box and select the name of the person making the request in the Client Contact dropdown list.
5. Ensure the Outstanding tickbox is ticked
6. Click Staff reminder and Future Staff reminder and enter a date three weeks forward. This will send you as the user an email in three weeks to ensure you have complied with the request and Click Save

When you have complied with the request you look up the activity for this client and you untick the Outstanding tickbox to indicate you have complied with the request. You can also add in additional notes in relation to the request in the comments section.

You can check if there are any GDPR SARS request outstanding at any stage as follows.

1. Click on reporting and Activity reporting
2. In the Activities Filter select GDPR in Level 1 and Select SARS Request in Level 2
3. Click the Outstanding tickbox as Yes and click Full report.
4. That will display any outstanding GDPR SARS requests.