ParishSOFT® | Accounting
A Part of the Ministry Brands® Family

ParishSOFT Accounting April 2019 Release Notes

These release notes inform you of new features, enhancements, and changes made in the April 2019 release of ParishSOFT Accounting.

Browser Compatibility

ParishSOFT Accounting supports the following browsers only:

- Internet Explorer, Version 9.0, 10.0, 11.0.

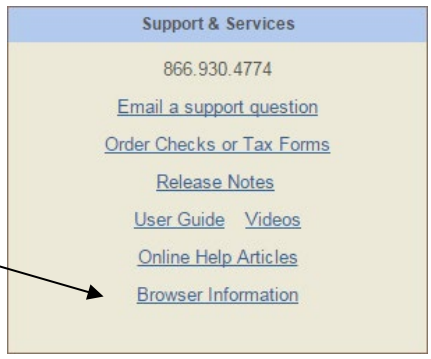
Note

If your browser is IE 10 or IE 11, when you display the ParishSOFT Accounting website, a message appears to inform you that the browser is not compatible with the site. To resolve this error message, turn on the browser's setting to Compatibility View.

- Microsoft Edge 41.16299.15.0 HTML 16.16299
- Firefox:
  - For PC, Version 40.0 or higher
  - For MAC, Version 40.0 or higher
- Safari, Version 9.0 or higher
- Chrome, Version 62.0 or higher

Additional Information

For information about recommended settings, IE's Compatibility View, and tips for using the various browsers, refer to our **Browser Information** page. To view this page, click the Browser Information link, located in the **Support & Services** section on your dashboard.



What's New

System-Wide

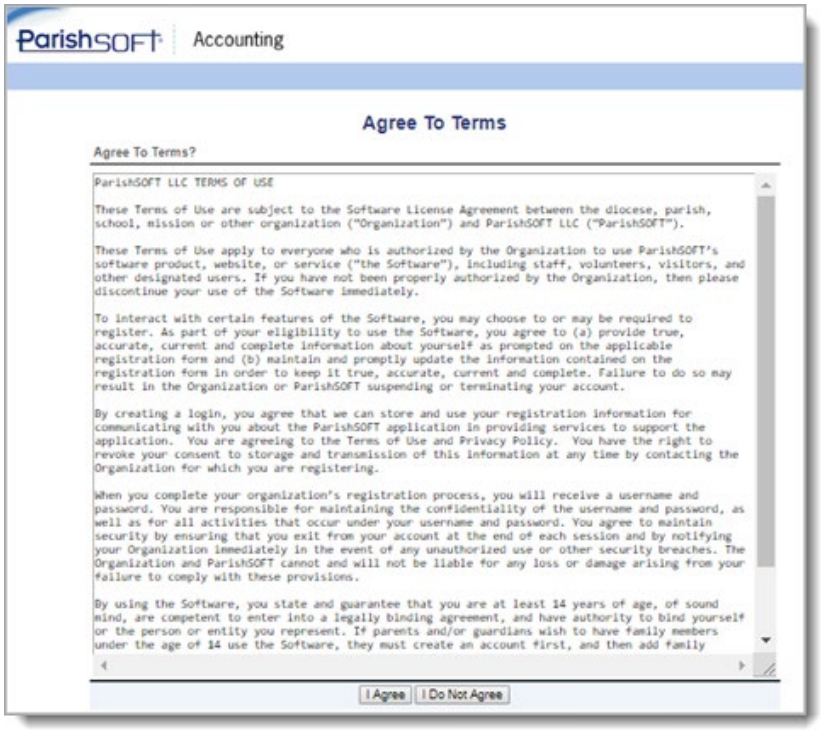
GDPR Compliance

On May 25, 2018 the European Union's General Data Protection Regulation (GDPR) went into full effect. GDPR is a European regulation that addresses data protection and privacy for individuals located in and outside of the European Union. The major focus of GDPR legislation is to give individuals control over their personal data collected and stored by businesses. The notes in this section describe functionality added to modules in the ParishSOFT Accounting to help make it easier for users of our software to comply with GDPR legislation.

Terms of Use Agreement Added for New and Existing Users

GDPR requires websites to disclose any data collection and give each user the ability to consent to having his or her personal data collected. To comply with the legislation, we updated our Terms of Use agreement and Privacy policy to give new and existing users the ability to consent to having ParishSOFT transmit and store personal information in their profile.

The updated Terms of Use agreement is shown below. Please read the agreement carefully. The new terms replace any previous terms set by ParishSOFT.

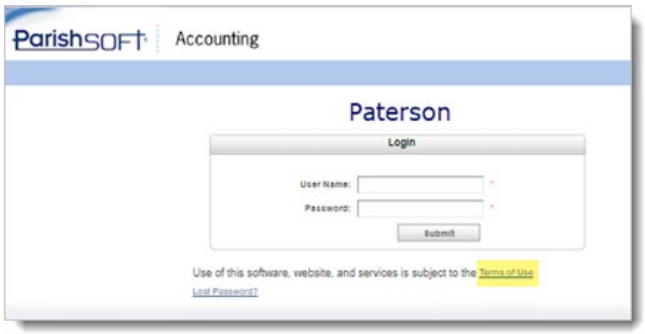


After reading the terms, indicate your agreement by selecting one of these buttons:

- I Agree: if you accept the terms and conditions, click this button. You are legally bound by the terms. You can proceed to access and use the site.
- I Do Not Agree: if you do not accept the terms and conditions, click this button. Your access to the site is prohibited. The system returns you to the **Login** page.

You have the right to revoke your consent to storage and transmission of this information at any time by contacting the church or organization in which you are registered.

We recommend that you periodically review the Terms of Use agreement. At any time, you can read the current agreement by clicking the Terms of Use link at the bottom of the ParishSOFT Accounting **Login** page:



Consolidation Manager

Options

Option Added to Activate the "Forget Records" Feature for Churches

GDPR legislation governs the collection, processing, and storage of personal data of individuals. One GDPR directive, the "Right to Be Forgotten", strengthens individuals' privacy rights by allowing them to request that organizations remove their personal data. In GDPR terms, personal data is any information that specifically identifies the individual, such as his or her name, address, and phone number.

In ParishSOFT Accounting, GDPR's "Right to Be Forgotten" feature is enabled in the Consolidation Manager module by using the **Enable GDPR Processes** option. This option was added to the bottom of the **Options** page:

By default, the **Enable GDPR Processes** option is disabled. When enabled, church administrators can use the Forget processes available in the ParishSOFT Accounting modules they are licensed to use, specifically:

- In Ledger and Payables, church administrators can use the Forget Vendor process to remove personal information from vendor records (see "Forget Vendor Feature Added" for details).
- In Accounts Receivable, church administrators can use the Forget Customer process to remove personal information from customer records (see "Forget Customer Feature Added" for details).
- In Payroll, church administrators can use the Forget Employee process to remove personal information from employee records (see "Forget Employee Feature Added" for details).

The **Enable GDPR Processes** option also controls access to features associated with each module's Forget process. For example, when the option is enabled, users of Ledger and Payables can generate a report listing the names of "forgotten" vendors. They can also view dates when vendors requested to have their personal information removed and when that information was actually removed.

Added Ability to Set the Password Change Policy for All Users

For security purposes, organization administrators can now set a password change policy that determines how long users are allowed to use a password before the system requires them to change it.

In the **Passwords** section, the new **Force Periodic Password Change Default** dropdown list contains options the administrator can select to globally set the default expiration frequency for user account passwords. Four options are available:

Note

The expiration frequency options listed below are presented in order from most secure to least secure.

- **Every 30 days**: (most secure) passwords expire and must be changed every 30 days.
- **Every 90 days**: passwords expire and must be changed every 90 days.
- **Yearly**: passwords expire and must be changed every 365 days.
- **Never**: (least secure) passwords never expire.

After the default expiration frequency is globally set, it takes effect immediately. The system does the following:

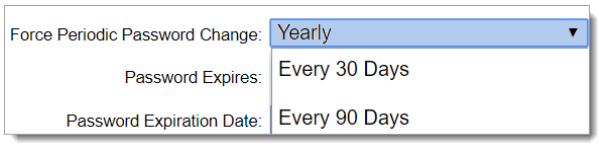
- Applies the default expiration frequency to each subsequently added new user account.
- Updates existing user accounts currently set to a less secure expiration frequency value (see previous list) to the new default value.

  For example, if **Every 90 days** is set as the new default, the password expiration frequency on all accounts currently set to **Yearly** or **Never** is changed to **Every 90 days**. If **Every 30 days** is selected as the new default, all accounts are set to **Every 30 days**.
- Retains the password expiration frequency on all existing user accounts if the frequency is currently set to a value equal to or more secure (see previous list) than the new default.

  For example, if **Yearly** is saved as the new default, the password expiration frequency is retained for all accounts currently set to **Yearly**, **Every 90 days**, or **Every 30 days**.

When the specified expiration date is reached, users are prompted to change the account password and must do so before being allowed to log in.

The globally set default password expiration frequency option controls which of the other frequency options appear in the associated **Force Periodic Password Change** dropdown list, located in each registered user's record. The system automatically updates this dropdown list depending on which frequency option the administrator set as the default. In the list, the default option is preselected, and the only other options included are those that are more secure than the default. Therefore, a user can accept the default or select a more secure expiration frequency for the account. The following illustration is provided to help you understand the behavior of the **Force Periodic Password Change** list:



In the above illustration, **Yearly**, the globally set default is preselected in the **Force Periodic Password Change** dropdown list. The only other frequency options that a user can select and apply to the account are those that are more secure than **Yearly**: **Every 90 days** and **Every 30 days**.

Ledger and Payables

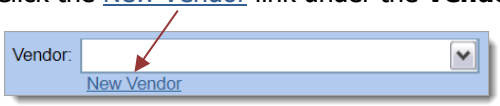
Credit Cards

Added the Ability to Add a Vendor Record

Now you can add a vendor on the fly to Ledger and Payables from the **Charge Information** page. Here's how:

1. Click 

to display the **Charge Information** page.
2. Click the New Vendor link under the **Vendor** dropdown list:



3. Complete the fields in the **New Vendor** form. When done, click Save.

   The vendor's record is added to your system.

Memorized

Controls Added to Prevent Users from Memorizing and Processing Certain Transactions

As a security measure, we added controls so that users cannot do the following:

- Memorize any transaction that includes an archived account.
- Process any memorized transaction that includes an archived account.

Additionally, users in organizations for which the **Hide Net Assets** option is enabled cannot perform these tasks:

- Memorize any transaction that includes a Net Asset account.
- Process any memorized transaction that includes a Net Asset account.

Moreover, users in organizations for which the **GAAP Compliance Function** is enabled cannot do the following:

- Memorize any transaction that includes a Dedicated account.
- Run any previously created memorized transaction that includes a Dedicated account.

Process

Forget Vendor Feature Added

Notes

Only users with Church Admin or Dio Admin permissions can use the Forget Vendor feature.

The Forget Vendor feature is available only if GDPR processes are enabled in the Consolidation Manager module.

Users with the appropriate permissions can now remove a vendor's personal data from their Ledger and Payables database. In GDPR terms, personal data means any data that can be used to specifically identify a vendor, such as the address and phone number.

If a vendor submits a request to have their personal data removed, do the following:

IMPORTANT

You cannot remove personally identifying data for any vendor with a transaction balance or any vendor receiving a 1099 in the current year.

1. Click Process.
2. Open the **Other Processes** group.
3. Select Forget Vendor.
4. In the **Forget Vendor** dropdown list, select the vendor whose data you want to remove.

WARNING

You are about to permanently remove the selected vendor's personally identifying information from your database. Before proceeding, verify that you selected the right vendor. After you click the Submit button, the vendor's personal information will be removed from your database and can no longer be retrieved.

5. Click Submit.

In compliance with GDPR data privacy regulations, all personally identifying information is removed from the vendor's record. To protect the vendor's identity, the **Name** field in the vendor's record now shows "GDPR."

To verify that the vendor's personal information was successfully removed, you can run a Forgotten Vendor List report. For details, see "Forgotten Vendor List Report Added".

Controls Added to Prevent Users from Merging Forgotten Vendor Records

As part of the implementation of the GDPR "Right to Be Forgotten" feature, we added controls to prevent users from merging records of vendors who requested that their personal data be removed.

Reports

Forgotten Vendor List Report Added

The **Standard Reports** group now includes the Forgotten Vendor List report. You can run this report to verify that the Forget Vendor process successfully removed a vendor's personal data from your database.

Note

The Forgotten Vendor List report is available only if GDPR processes are enabled in the Consolidation Manager module.

To run this report:

1. Click 

. Then, in the **Standard Reports** group, open the **Vendors** group.
2. Select Forgotten Vendor List.
3. On **Configure Report** page, set up the report by doing the following:
    - Select a date range for the report by entering a date in the **Start Date** and **End Date** fields. If you want a report for a specific day, enter the same date in both fields.
    - If desired, specify a subtitle for the report by entering a title in the **Report Subtitle** field.
4. Click the desired report buttons to generate and view the list of forgotten customers.

Accounts Receivable

Process

Forget Customer Feature Added

Notes

Only users with Church Admin or Dio Admin permissions can use the Forget Customer feature.

The Forget Customer feature is available only if GDPR processes are enabled in the Consolidation Manager module.

We added a feature that enables users with the appropriate permissions to remove a customer's personal data from the database. In GDPR terms, personal data means any data that can be used to specifically identify a customer, such as the name and phone number.

If a customer submits a request to have their personal data removed, do the following:

IMPORTANT

You cannot remove personally identifying data for any customer with a balance or transactions in the current year.

1. Click 

.
2. Select Forget Customer.
3. In the **Forget Customer** dropdown list, select the customer whose data you want to remove.

WARNING

You are about to permanently remove the selected customer's personally identifying information from your database. Before proceeding, verify that you selected the right customer. After you click the Submit button, the customer's personal information will be removed from your database and can no longer be retrieved.

4. Click Submit.

In compliance with GDPR data privacy regulations, all personally identifying information is removed from the customer's record. To protect the customer's identity, the **Name** field in the customer's record now shows "GDPR."

To verify that the customer's personal information was successfully removed, you can run a Forgotten Customer List report. For details, see "Forgotten Customer List Report Added".

Reports

Forgotten Customer List Report Added

The **Standard Reports** group now includes a Forgotten Customers List report. You can this report to verify that the Forget Customer process successfully removed a customer's personal data from your database.

Note

The Forgotten Customer List report is available only if GDPR processes are in the Consolidation Manager module.

To run this report:

1. Click 

.
2. In the **Standard Reports** group, open the **Customers** group.
3. Select Forgotten Customer List.
4. On **Configure Report** page, set up the report by doing the following:
   - Select a date range for the report by entering a date in the **Start Date** and **End Date** fields. If you want a report for a specific day, enter the same date in both fields.
   - If desired, specify a subtitle for the report by entering a title in the **Report Subtitle** field.
5. Click the desired report buttons to generate and view the list of forgotten customers.

Payroll

Process

Forget Employee Feature Added

Notes

Only users with Church Admin or Dio Admin permissions can use the Forget Employee feature.

The Forget Employee feature is available only if GDPR processes are enabled in the Consolidation Manager module.

We added a feature that enables users with the appropriate permissions to remove an employee's personal data from the Payroll database. In GDPR terms, personal data means any data that can be used to specifically identify a customer, such as the name and phone number.

If an employee submits a request to have their personal data removed, use the following procedure:

IMPORTANT

You cannot remove personally identifying data for any employee who has a record of receiving a pay check within the last seven years.

1. Click Process.
2. Select Forget Employee.
3. In the **Forget Employee** dropdown list, select the employee whose data you want to remove.

WARNING

You are about to permanently remove the selected employee's personally identifying information from your database. Before proceeding, verify that you selected the right employee. After you click the Submit button, the employee's personal information will be removed from your database and can no longer be retrieved.

4. Click Submit.

In compliance with GDPR data privacy regulations, all personally identifying information is removed from the employee's record. To protect the employee's identity, the **Name** field in the employees' record now shows "GDPR."

To verify that the employee's personal information was successfully removed, you can run a Forgotten Employee List report. For details, see "Forgotten Employee List Report Added".

Reports

Forgotten Employee List Report Added

We added a Forgotten Employee List report. This report lets you generate a list of employees whose personally identifying information was removed from your system. You can run this report to verify that the Forget Employee process successfully removed an employee's personal data from your database.

To run this report:

Note

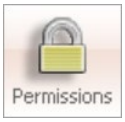
The Forgotten Employees List report is available only if GDPR processes are enabled in the Consolidation Manager module.

1. Click 

.
2. In the **Standard Reports** group, open the **Employees** group.
3. Select Forgotten Employee List.
4. On **Configure Report** page, set up the report by doing the following:
   - Select a date range for the report by entering a date in the **Start Date** and **End Date** fields. If you want a report for a specific day, enter the same date in both fields.
   - If desired, specify a subtitle for the report by entering a title in the **Report Subtitle** field.
5. Click the desired report buttons to generate and view the list of forgotten employees.

Resolved Issues

Church Manager



Permissions

CNACT-1361 Permissions Prior Period Adjustments Field

Previously in the **Ledger and Payables** group, the checkbox for the **Prior Period Adjustments** permission was selected by default in records of new users assigned the role of **Church User**. Per customer request, we changed the default value to the deselected state. Now, Diocesan Admin users can assign this permission to new users on a case-by-case basis.