

EBOOK

# CCPA Readiness using Sage 100cloud

*How features and tools in Sage 100cloud can assist you in securing consumer data*



# Contents

## **A Quickstart Guide to the California Consumer Privacy Act**

Kier Thomas-Bryant

## **How Sage 100cloud can help businesses comply with the CCPA**

Linda Cade

### **Sage legal disclaimer**

*The information contained herein is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. We would like to stress that there is no substitute for customers making their own detailed investigations or seeking their own legal advice if they are unsure about the implications of the California Consumer Privacy Act (CCPA) on their businesses.*

*While we have made every effort to ensure that the information provided herein is correct and up to date, Sage makes no promises as to completeness or accuracy and the information is delivered on an "as is" basis without any warranties, express or implied. Sage will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using this information.*



Considering that many US and even worldwide businesses ship products to California, or have online properties like websites that are available to Californians, a significant number of businesses will need to make timely preparations, and ensure ongoing compliant processes are in place.

# A Quick Start Guide to the The California Consumer Privacy Act (CCPA)

**Kier Thomas-Bryant**

*Originally published to Sage Advice on August 7, 2019 as "The California Consumer Privacy Act: A quick start guide"*

Starting January 1, 2020, new California protection for personal information comes into effect that directly affects some businesses that offer products or services to consumers in the state.

The California Consumer Privacy Act of 2018 (CCPA) aims to protect the personal information of California consumers, in a similar although not identical way to the General Data Protection Act (GDPR) in European countries.

The CCPA therefore introduces significant requirements for businesses that fall within its scope.

Considering that many US and even worldwide businesses ship products to California, or have online properties like websites that are available to Californians, a significant number of businesses will need to make timely preparations, and ensure ongoing compliant processes are in place.

Below we answer some frequently asked questions about the CCPA that might help kick start your preparedness plans. This is not a substitute for legal advice. We advise you consult the legislation yourself to find out how it impacts your business. You might also seek the advice of a data protection expert, or consult the California Attorney General directly for an opinion on how to comply (a right that is provisioned under the act).

## What is the CCPA?

In broad terms the CCPA is a continuation of the California Constitution that says the right to privacy is inalienable. It forms part of California privacy legislation, which includes other legislation such as the Online Privacy Protection Act (CalOPPA), the Privacy Rights for California Minors in the Digital World Act, and—in particular—Shine the Light, which gives Californians the right to know how businesses handle their personal information.

Again in broad terms, the CCPA specifically gives California consumers the right to know the following from businesses that conduct commercial activities in the state:

- What personal information is being collected about them
- Whether their personal information is sold or disclosed—and to whom

It gives them the right to:

- Say no to the sale of personal information, and request it is deleted
- Request a copy of their personal information held by a business
- Not be discriminated against in price or product/services offered should they exercise their rights under the CCPA

Affected businesses (see below) need to put in place measures to ensure the above is possible.

## When does the CCPA take effect?

The CCPA becomes law on January 1, 2020.

## What kinds of businesses or organizations does the CCPA affect?

The CCPA applies to any business that can be described in any or all of the following ways:

- Has annual gross revenues in excess of \$25,000,000

- That alone or in combination with another business, buys or sells the personal information of 50,000 or more consumers, households, or devices
- Derives 50% or more of its annual revenues from selling consumers' personal information

Additionally, the CCPA applies to any entity controlled by any of the types of business described above, and that shares common branding with the business.

## What kinds of businesses or organizations are exempt from the CCPA?

A business does not fall under the scope of the legislation if it has gross revenues of \$25,000,000 or less, or does not buy or sell the personal information of consumers, households, or devices. If the business buys or sells the personal information of less than 50,000 consumers, households or devices then it also does not fall under the scope of the legislation.

Some charities, social enterprises, not-for-profit organizations, or non-governmental organizations (NGOs) fall outside the scope of the CCPA provided they are not operated for the profit or financial benefit of their shareholders or other owners, and they are not incorporated into a legal entity such as a sole proprietorship, partnership, LLC, corporation, or association (or are controlled by such a business, including sharing branding).

## What does the CCPA mean for my business?

The CCPA imposes a number of requirements on eligible businesses in order to comply, with the following being prime examples:

- **Enabling consumer disclosure requests:** There must be two or more ways made available to consumers for them to submit requests for personal information disclosure. At the very least, these must be a toll-free telephone number and a website address (if the business operates a website).

- **Disclosure requirements:** Information disclosed following a request from a consumer should cover the 12-month period preceding the date of the request and—as with the GDPR—should be in a readily-usable format that “allows the consumer to transmit [the] information from one entity to another entity without hindrance”. This includes a so-called “look back” requirement, that predates the CCPA’s introduction. In other words, businesses are already required to maintain records conforming to the CCPA’s requirements, all the way back to January 1, 2019. The consumer cannot be required to create an account with the business in order to make a request. Any personal information provided to verify the disclosure request should be used solely for the purposes of verification. There cannot be a charge for this disclosure.
- **Timely disclosure:** Once a request has been received from a consumer, the information must be supplied within 45 days. This can be extended a single time by a further 45 days when “reasonably necessary” although the consumer must be provided with notification of the extension within the first 45 day period. Verifying the consumer’s request as genuine should not delay the process, so it effectively has to occur within the initial 45 day period.
- **Opt-out requests:** There must be a process by which consumers can instruct businesses that sell data to third parties not to sell their personal information (see “Do my business’ privacy or data protection policies need to be updated for the CCPA?” below). A consumer is able to reverse this decision by providing subsequent express authorization for the business to sell their personal information, but the business can’t approach the consumer to do so until 12 months have passed after the initial opt-out.
- **Minors opt-in:** Processes must be in place to block the sale of personal information for a consumer for whom the business has actual knowledge is less than 16 years of age. However, consumers aged between 13 and 16 years of age (or their parents/guardian) can affirmatively authorize the sale of personal information (the CCPA calls this the “right to opt-in”). A policy of deliberate ignorance about the age of minors by businesses will be interpreted as the business having had actual knowledge of their age and, therefore, should be avoided.
- **Deletion requests:** There must be a process by which personal information collected for a consumer can be deleted by the business or their service providers. However, the business does not necessarily have to comply, given specific circumstances—see “Do I have to delete data for the CCPA?” below.
- **Updated privacy policies:** Online privacy policies (or any other description of California-specific consumer rights) should be updated in time for January 1, 2020 and then updated at least once every 12 months subsequently. For more details of what should be included, see “Do my business’ privacy or data protection policies need to be updated for the CCPA?” below. If your business begins to collect additional categories of personal information then it should be instantly reflected in the policies.
- **Website changes:** If the business has a website then it must show a clear and conspicuous link entitled, “Do Not Sell My Personal Information”. This should link to a web page that lets consumers opt-out of the sale of their personal information. It should not be required for the consumer to create an account to opt-out. By taking “reasonable steps”, businesses can redirect California consumers to a specific version of their website that includes the “Do Not Sell My Personal Information” link and CCPA information, avoiding the need for all website visitors to see them.
- **Staff training:** All individuals responsible for handling consumer inquiries about privacy practices or compliance need to be informed about the CCPA’s requirements. They need to know how to direct consumers to exercise their rights under the CCPA.

## What data can California consumers request under the CCPA?

If a business collects or sells personal information about a consumer then that consumer has the right to request a business disclose the information listed below, covering the 12 months prior to the request (which should be verified as genuine).

If a business collects personal information about the consumer, they should disclose:

- The categories of personal information it has collected about that consumer.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting or selling personal information.
- The categories of third parties with whom the business shares personal information.
- The specific pieces of personal information it has collected about that consumer.

If a business sells personal information about the consumer (or discloses it for a business purpose), they should disclose the following:

- The categories of personal information that the business collected about the consumer.
- The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information. This should be split out according to each third party to whom the personal information was sold.
- The categories of personal information that the business disclosed about the consumer for a business purpose.

If personal information in any category has not been sold or disclosed for a business purpose then this should be stated in response to the request.

## Does my business have to collect additional personal information for the CCPA?

No. For businesses that collect personal information, the CCPA doesn't require them to retain information for a single one-time transaction if it wouldn't ordinarily. Nor does it require businesses to re-identify or otherwise link any data that ordinarily is not maintained in a way that would be considered personal information.

## Does my business have to delete personal information for the CCPA?

The CCPA doesn't change or place restrictions on the kinds of personal information that can be stored by businesses.

However, the CCPA does allow consumers to request a business or its service providers delete personal information relating to them. As with requests for personal information disclosure, the business should verify the request is genuine before taking action.

Notably, a business can refuse to comply with a deletion request for any of the following reasons:

- The personal information is required to complete a transaction for which the data was collected, such as providing a good or service requested by the consumer.
- The business reasonably anticipates they will provide a good or service to the consumer, for which the data was collected, or otherwise perform a contract between business and consumer.
- The personal information enables solely internal uses that are reasonably aligned with the expectations of the consumer based on their relationship with the business.
- The personal information is used to detect security incidents, or protect against malicious, deceptive, fraudulent, or illegal activity (or the personal information is required to prosecute those responsible).
- The personal information is required to debug, identify or repair errors that impair existing intended functionality.
- The personal information is required to exercise free speech (both for the business or consumer).
- The personal information is required to exercise another right provided for by law, or to comply with a legal obligation.

- The personal information is required to exercise another right provided for by law, or to comply with a legal obligation.
- The personal information is required to comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
- The personal information is required to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest.

It's also noted within the CCPA that the business can refuse to comply with the deletion request if it otherwise uses the personal information internally in a lawful manner that's compatible with the context in which the consumer provided the information.

## Who can request disclosure of information or request deletion of information under the CCPA?

Any natural person who is legally defined as a California resident, which in broad terms is every individual who is in the State for other than a temporary or transitory purpose, and every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose.

## Can my business opt out of the CCPA?

Not if any commercial conduct takes place in California. You should not treat consumers who exercise their rights under the CCPA any differently. To do so is considered unlawful discrimination and examples might include denying consumers goods or services, charging different prices or rates (or suggesting different prices or rates will apply), or providing a different level of quality of goods or services.

## Is the CCPA the same as the GDPR?

It's similar in spirit to the GDPR but, generally speaking, the CCPA has a narrower and more specific focus compared to the GDPR.

The GDPR places restrictions on how companies collect and handle personal data, bring about transparency, and provides individuals with rights over that data. It is limited to digital data.

The CCPA is solely concerned with providing rights to consumers regarding their personal information (digital or otherwise), and demanding transparency from businesses. The requirements it places upon businesses are simply to facilitate this, and to ensure consumers are aware of their rights. The CCPA covers all personal information that a business might hold, digital or otherwise.

Some of the work done by a business to comply with the GDPR will likely mean that it's compliant with the CCPA, but this is not guaranteed and the CCPA has additional and specific requirements that require significant additional actions.

## Does the CCPA let my business sell the personal information of consumers?

Businesses can sell personal information they have collected about consumers.

However, before they sell information they have bought from another business, they must explicitly inform the consumer and provide them with an opportunity to opt out.

## If my business is outside California, do I have to comply with the CCPA?

The CCPA doesn't apply to a business that collects or sells a non-California consumer's personal information provided every aspect of that commercial conduct takes place wholly outside of California (and this includes the consumer being outside California at the time).

Nor does the CCPA restrict a business' ability to comply with federal, state or local laws.

Simply ask yourself the question: Are the services or products my business offers available in California? Even if a business is located in another state (or even outside the US), if its services are available in California or products can be shipped there then the CCPA probably applies. For example, websites can typically be accessed by anybody worldwide, so even a website in Europe or Russia arguably could be required to make adaptations (although with the use of geo IP redirection it might be possible to provide a version of your website specifically for California residents).

## Can my business be fined if it violates the CCPA?

California consumers can take action against businesses that violate the CCPA in order to seek damages. Examples of violations could include “unauthorized access and exfiltration, theft, or disclosure of a consumer’s nonencrypted or nonredacted personal information.”

Consumers can recover damages of not less than \$100, but not greater than \$750 per consumer, per incident. However, a court can apply declaratory relief and any other relief it deems proper, as well as injunctive relief.

The California Attorney General can also take civil action on behalf of the people of California, including imposing an injunction and a civil penalty of civil penalty of \$2,500 for each violation or up to \$7,500 for each intentional violation.

Once informed of a violation, which must be done in writing, businesses have 30 days to fix it before they are considered to have violated the CCPA.

## Do my business’ privacy or data protection policies need to be updated for the CCPA?

Yes. Such policies need to include the following, at a minimum:

- A description of consumer rights as provided by the CCPA relating to disclosure or personal information, opting out, and deletion of relevant personal information by the business or its service providers.

- A link to the “Do Not Sell My Personal Information” page on the business’ website (if the business has a website).
- A statement about how the business will not discriminate against consumers who exercise their rights under the CCPA.
- Two separate lists, and within the wording of the CCPA there are rules about what data should be listed, and how it should be organized. The legislation should therefore be consulted before taking action. However, in broad terms the first list should display categories of personal information the business has sold about consumers in the preceding 12 months. The second should list categories of personal information disclosed about consumers for a business purpose in the preceding 12 months. In the event there has been no personal information sold or disclosed for a business purpose then this should be stated.

## Can my business charge a fee for a consumer request under the CCPA?

No.

## Can my business take action against consumers who abuse the CCPA?

Businesses are not obligated to provide information to the same consumer more than twice in a 12-month period.

*Note: We would like to stress that there is no substitute for customers making their own detailed investigations or seeking their own legal advice if they are unsure about the implications of the California Consumer Privacy Act (CCPA) on their businesses.*

- **Disclosure requirements:** Information disclosed following a request from a consumer should cover the 12-month period preceding the date of the request and—as with the GDPR—should be in a readily-usable format that “allows the consumer to transmit [the] information from one entity to another entity without hindrance”. This includes a so-called “look back” requirement, that predates the CCPA’s introduction. In other words, businesses are already required to maintain records conforming to the CCPA’s requirements, all the way back to January 1, 2019. The consumer cannot be required to create an account with the business in order to make a request. Any personal information provided to verify the disclosure request should be used solely for the purposes of verification. There cannot be a charge for this disclosure.
- **Timely disclosure:** Once a request has been received from a consumer, the information must be supplied within 45 days. This can be extended a single time by a further 45 days when “reasonably necessary” although the consumer must be provided with notification of the extension within the first 45 day period. Verifying the consumer’s request as genuine should not delay the process, so it effectively has to occur within the initial 45 day period.
- **Opt-out requests:** There must be a process by which consumers can instruct businesses that sell data to third parties not to sell their personal information (see “Do my business’ privacy or data protection policies need to be updated for the CCPA?” below). A consumer is able to reverse this decision by providing subsequent express authorization for the business to sell their personal information, but the business can’t approach the consumer to do so until 12 months have passed after the initial opt-out.
- **Minors opt-in:** Processes must be in place to block the sale of personal information for a consumer for whom the business has actual knowledge is less than 16 years of age. However, consumers aged between 13 and 16 years of age (or their parents/guardian) can affirmatively authorize the sale of personal information (the CCPA calls this the “right to opt-in”). A policy of deliberate ignorance about the age of minors by businesses will be interpreted as the business having had actual knowledge of their age and, therefore, should be avoided.
- **Deletion requests:** There must be a process by which personal information collected for a consumer can be deleted by the business or their service providers. However, the business does not necessarily have to comply, given specific circumstances—see “Do I have to delete data for the CCPA?” below.
- **Updated privacy policies:** Online privacy policies (or any other description of California-specific consumer rights) should be updated in time for January 1, 2020 and then updated at least once every 12 months subsequently. For more details of what should be included, see “Do my business’ privacy or data protection policies need to be updated for the CCPA?” below. If your business begins to collect additional categories of personal information then it should be instantly reflected in the policies.
- **Website changes:** If the business has a website then it must show a clear and conspicuous link entitled, “Do Not Sell My Personal Information”. This should link to a web page that lets consumers opt-out of the sale of their personal information. It should not be required for the consumer to create an account to opt-out. By taking “reasonable steps”, businesses can redirect California consumers to a specific version of their website that includes the “Do Not Sell My Personal Information” link and CCPA information, avoiding the need for all website visitors to see them.
- **Staff training:** All individuals responsible for handling consumer inquiries about privacy practices or compliance need to be informed about the CCPA’s requirements. They need to know how to direct consumers to exercise their rights under the CCPA.

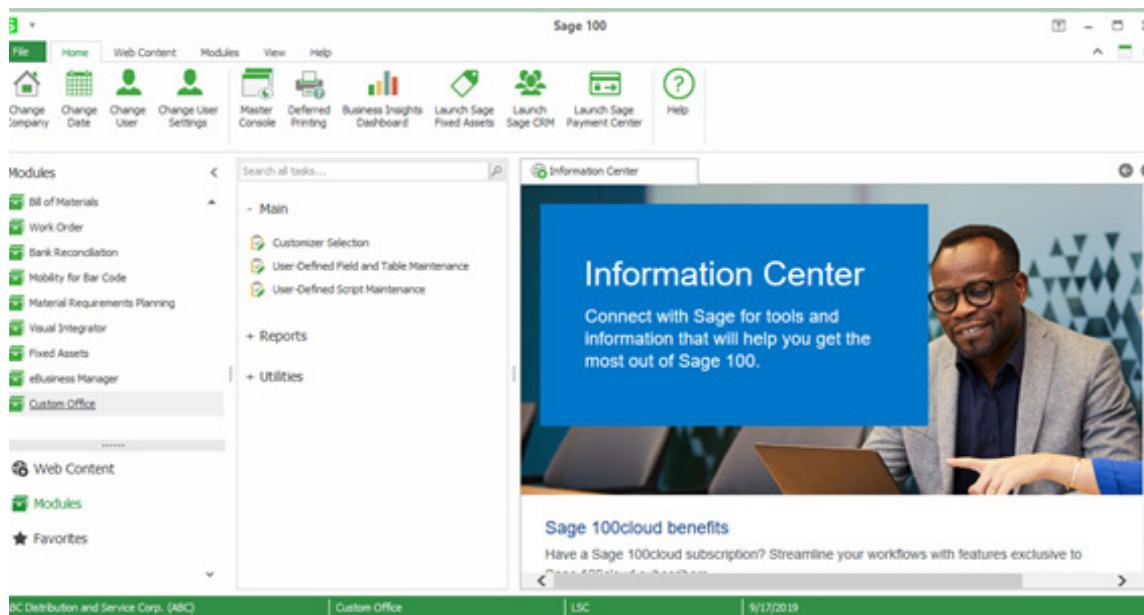
# How Sage 100cloud can help Businesses Comply with the CCPA

Linda Cade

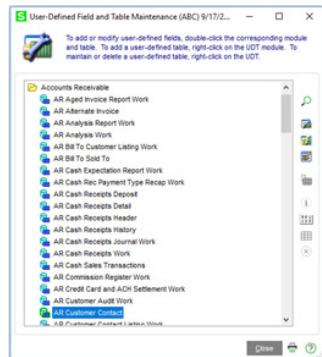
## Adding a User-Defined Field

In order to comply with the requirements of the California Consumer Privacy Act (CCPA), you may find you need some additional tracking, specific to personal information and how it is shared. Sage 100 Custom Office includes tools to assist you in doing just that. You may, for instance wish to add a special flag to identify consumers' information that is routinely sold or shared as part of your business process.

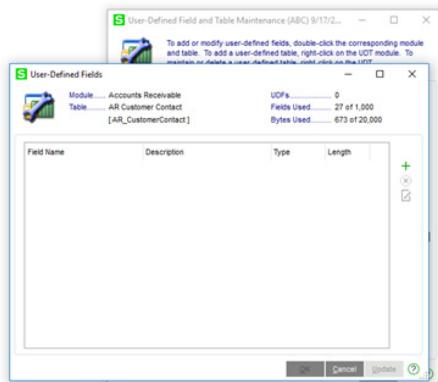
**1. Using Custom Office, from the Main menu, select User-Defined Field and Table Maintenance.**



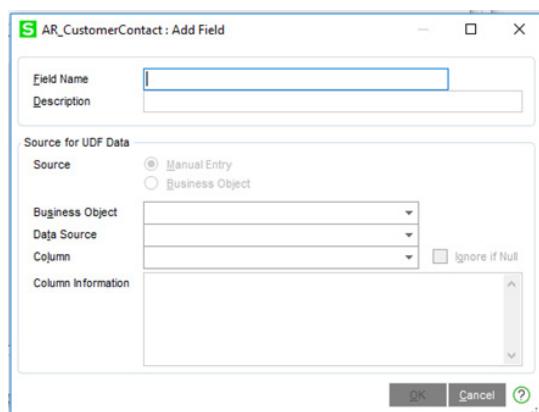
## 2. Select Accounts Receivable, AR Customer Contact



## 3. Click on the "+" button

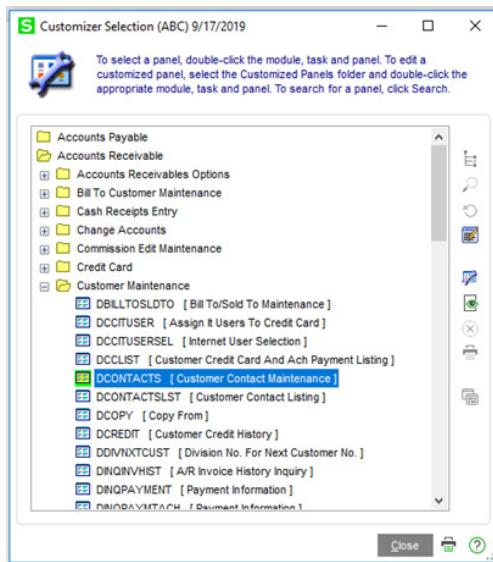


## 4. Enter a field name and define the User Defined Field (UDF) as a checkbox.

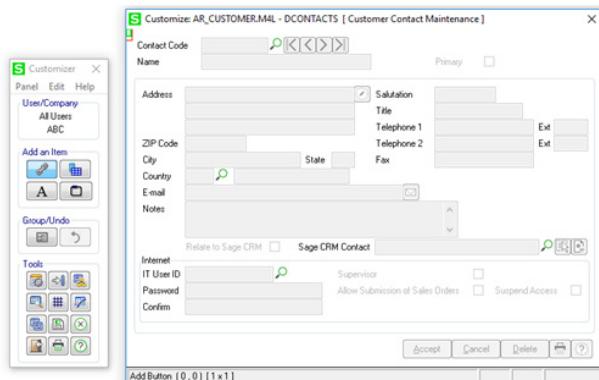


## 5. Complete the process to add the UDF and update the data tables.

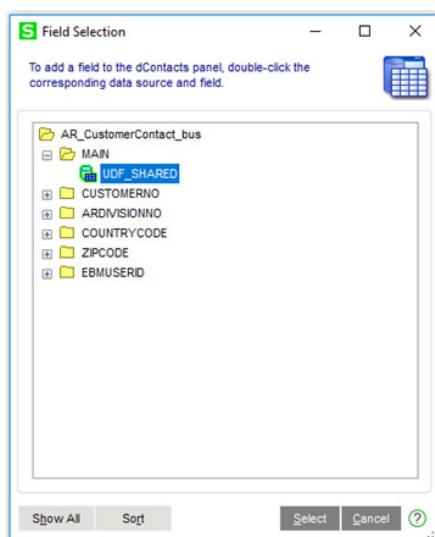
**6. From Custom Office, select Customizer Selection, Accounts Receivable, Customer Maintenance, DCONTACTS**



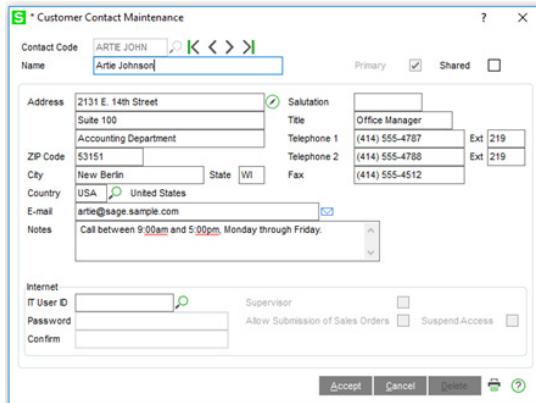
**7. Right-click and select Edit Panel. Select the appropriate User and Company. Then click "OK".**



**8. Click on the "Add Field"  button. Draw the field on the panel and select the UDF from the Field Selection screen.**



## 9. Exit and Save. You have now added a checkbox to the Customer Contacts Panel.

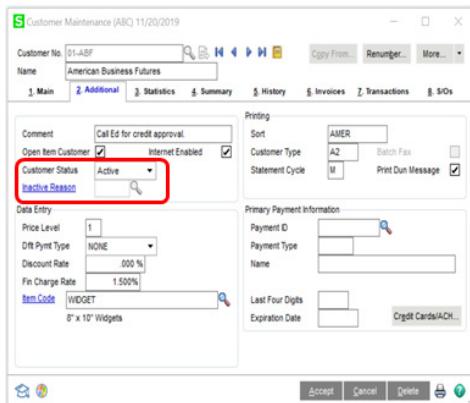


The screenshot shows the 'Customer Contact Maintenance' window. At the top, there is a contact code 'ARTIE JOHN' and a name 'Archie Johnson'. Below this, there are fields for address, ZIP code, city, country, and various telephone and fax numbers. A 'Notes' section contains the instruction 'Call between 9:00am and 5:00pm, Monday through Friday.' At the bottom, there are sections for 'Internet' (IT User ID, Password, Confirm) and 'Supervisor' (checkboxes for 'Allow Submission of Sales Orders' and 'Suspend Access'). A 'Shared' checkbox is located in the top right corner of the main data area. Buttons for 'Accept', 'Cancel', 'Delete', and a printer icon are at the bottom right.

## Inactivating and Deleting Consumer Data

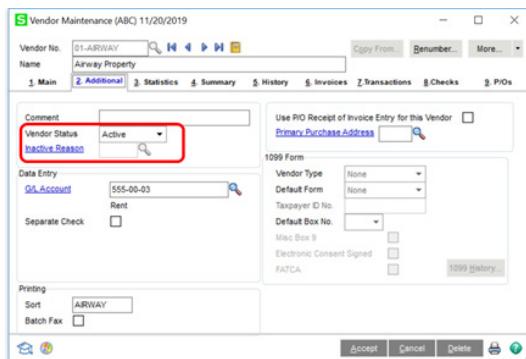
One of the most crucial tasks related to Consumer Privacy, and the “right to be forgotten”, is the removal of consumer data. There are stated exceptions, allowing for the retention of data beyond the initial request, allowing for completion of transactions, auditing, legal disputes, and the like. Nonetheless, at some point you will need a way to delete or de-identify data regarding a consumer if requested to do so. Sage 100 includes tools to assist you in that process as well. Once there is a determination that business has concluded with the consumer, the associated account should be tagged as “Inactive”. An Inactive Reason may also be selected.

### Inactive Customer



The screenshot shows the 'Customer Maintenance' window for customer '01-ABF' named 'American Business Futures'. The 'Additional' tab is selected. In the 'Customer Status' dropdown, 'Active' is selected. Below it, there is a 'Inactive Reason' search field. Other sections include 'Comment' (with 'Call Ed for credit approval.'), 'Data Entry' (with fields for Price Level, DFT Pmt Type, Discount Rate, and Fin Charge Rate), and 'Primary Payment Information' (with fields for Payment ID, Payment Type, Name, and Last Four Digits). Buttons for 'Accept', 'Cancel', 'Delete', and a printer icon are at the bottom right.

### Inactive Vendor



The screenshot shows the 'Vendor Maintenance' window for vendor '01-AIRWAY' named 'Airway Property'. The 'Additional' tab is selected. In the 'Vendor Status' dropdown, 'Active' is selected. Below it, there is a 'Inactive Reason' search field. Other sections include 'Comment' (with 'Use PO Receipt of Invoice Entry for this Vendor' checkbox), 'Data Entry' (with 'Q1 Account' set to '555-00-03' and 'Rent' checked), '1099 Form' (with dropdowns for Vendor Type, Default Form, Taxpayer ID No., and Default Box No.), and 'Printing' (with 'Sort' set to 'AIRWAY' and 'Batch Fax' checked). Buttons for 'Accept', 'Cancel', 'Delete', and a printer icon are at the bottom right.

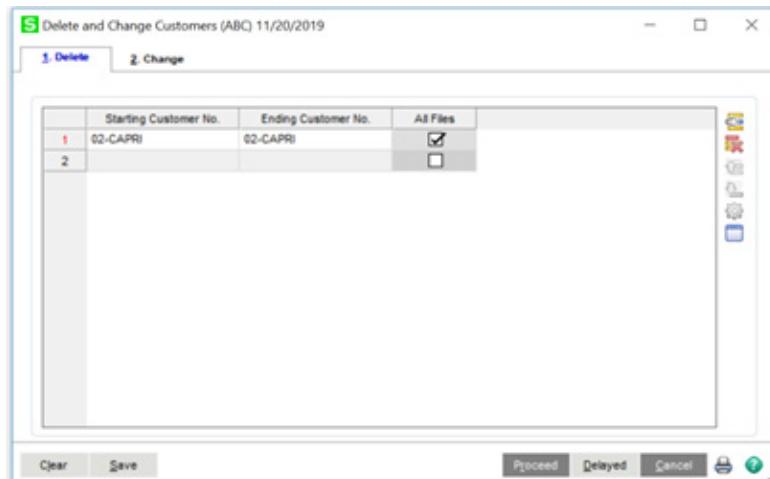
Once the consumer record is marked as "Inactive", it may be desirable for business reasons to allow some time to pass to allow for all transaction and reporting to be completed (Example: Vendor 1099 reporting). This status will flag the account and discourage further use for future entries.

Once satisfied that the records are no longer required, the consumer record can be deleted.

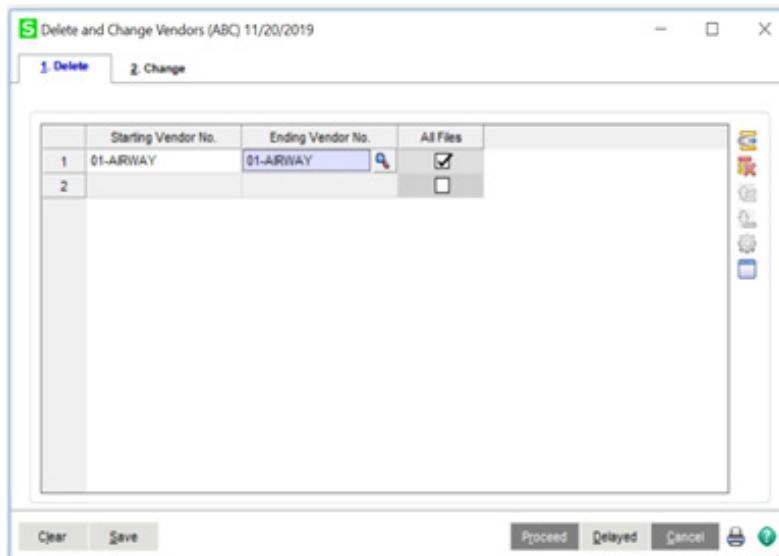
**WARNING: Use of these utilities will PERMANENTLY DELETE the selected records and all history associated with the account. Use of the utility should be limited to AUTHORIZED PERSONNEL. A VERIFIED BACKUP of the system is required to restore data in the event of inadvertent deletion.**

- For customer records, from the Accounts Receivable menu, Select Utilities. Under the Utilities menu, select Delete and Change Customers.
- For vendor records, from the Accounts Payable menu, Select Utilities. Under the Utilities menu, select Delete and Change Vendors.

### Delete and Change Customers

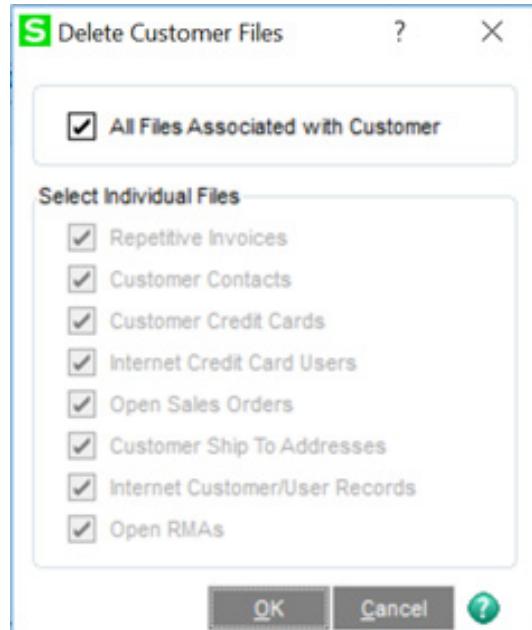


### Delete and Change Vendors

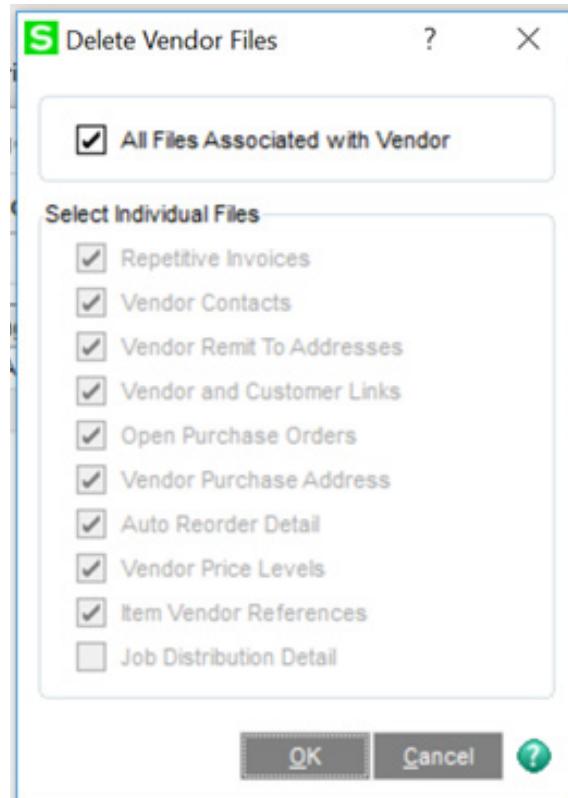


After having selected the correct Customer or Vendor ID's, click the Select Files  button to see a list of the files to be included in the process and change the settings for individual files as needed.

### Delete Customer Files



### Delete Vendor Files





Contact Us: 800.627.9032 | <https://www.dsдинc.com/contact/>

Contact Sage for more information

Sage (US) Limited  
271 17th Street Northwest  
Atlanta, GA 30363

[www.sage.com/ccpa](http://www.sage.com/ccpa)

©2020 The Sage Group plc or its licensors. Sage, Sage logos, Sage product and service names mentioned herein are the trademarks of The Sage Group plc or its licensors. All other trademarks are the property of their respective owners. NA/WF 183498.

