Redacting information

Redaction is the process of blanking out information on a document before it is released. This applies to individual words, sentences or whole sections of a document. Redaction should be done by a person who has knowledge of the subject matter to decide which material should be exempt.

When redaction is used on Freedom of Information requests (FOI) or Environmental Information Regulations requests (EIR) you need to explain to the applicant which exemptions have been applied and why. Redaction might also be needed when dealing with subject access requests.

Redaction guidance

You should always carry out redaction on a copy of the document, leaving the original intact. Never redact the master or original version of an electronic record – make a copy.

Delete any intermediate versions and only keep the original and the redacted version of the document.

Spacing should not indicate the missing information. Words should not be visible or be able to be guessed at due to incomplete redaction. Hold the paper up to the light to check.

Hard copy

Photocopy the original and block out the sensitive material using a black marker pen or quality correction fluid. Photocopy the document again for release.

Electronic documents

Make a copy, remove all the sensitive information and replace it with **[redacted]**. Print the redacted version. If an electronic version is needed, scan in the printed version as a pdf.

In Microsoft Office (Word, Excel, PowerPoint), you **must not** use the highlighter tool to highlight the text in black to 'hide' it. The highlighter tool does not properly redact information.

If the highlighter tool has been used, copying and pasting can reveal the sensitive information even if the document has been converted to a PDF.

PDFs

You can redact from PDFs if you have Adobe Acrobat Pro.

Make an electronic copy using Adobe Acrobat. Use the text touch-up tool to replace the redacted information with a redaction marker [redacted]. For help with this see the Adobe Acrobat redaction guidance or email the central scanning unit.

Word documents

Make an electronic copy and remove all sensitive information. Replace it with **[redacted]**. Print the document as a pdf – this is the redacted document.

Spreadsheets

Make an electronic copy by exporting the document as a .csv format file and remove all sensitive information. Replace it with **[redacted]**. The redacted version can be reimported to the spreadsheet.

Help and support

The data protection and information assets team can advise on all aspects of data protection:

- email data protection and information assets

Using redaction in Adobe® Acrobat® X

Best practices for removing sensitive text and images from documents

Table of contents

Redaction is the permanent deletion of visible text and images from documents. In the past, a black marker was used to hide sensitive information. These days, it doesn't make sense to print out a document just to redact it. The process is slow, expensive, and inefficient. Instead, law firms, government agencies, and organizations around the world rely on Adobe Acrobat Pro software to safely and permanently remove content from the document data stream.

Acrobat redaction tools were introduced in version 8, and redaction capabilities have continued to improve with each release. In Acrobat X Pro, several new redaction features were introduced:

- Redaction across pages—Repeat a redaction through a document. Useful for redacting headers and footers from documents.
- Partial pattern redaction—Mark part of a pattern for redaction. For example, mark part of a national ID or credit card number. Useful for identifying individuals without revealing personal information.
- Redaction mark appearance—Set the appearance of redaction marks. For example, mark items with a transparent red overlay.
- Overlay text in Comments list—View overlay text in the Comment list for quick review.

This paper provides tips for getting started and best practices for using the redaction tools in Acrobat X. Topics covered include:

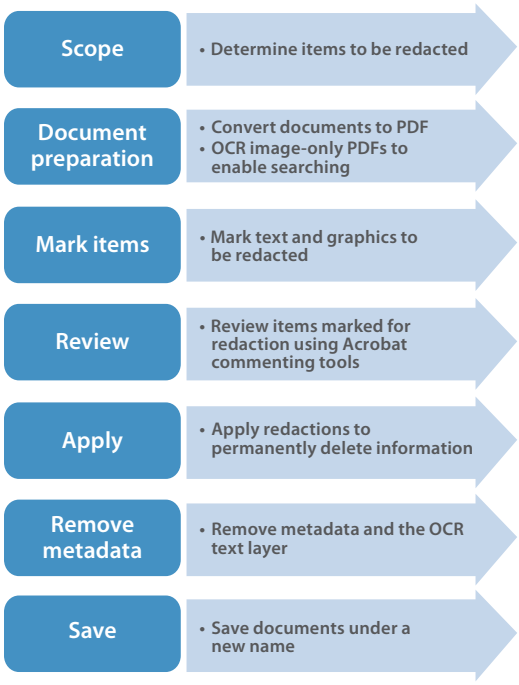
- Setting redaction preferences
- Marking text and graphics for redaction
- Setting common redaction properties
- Adding overlay text and exemption codes to a redaction
- Creating a report of redactions
- Applying redactions to permanently remove information
- Using Actions to automate the redaction workflow

Preparing for redaction

Redactions must be carefully applied and managed. Here are a few tips to get ready.

- Copy the documents to be redacted to a new folder on your hard drive.
- If the document is a scanned image, convert the image to searchable text using optical character recognition (OCR).
- Review the documents to identify the type of information that needs to be redacted. For example, personally identifiable information (PII), such as driver's license, national identification, or credit card numbers that can be used to identify, contact, or locate a person; names of companies or people that need to remain confidential; or trade secrets such as formulas or computer code.

The following diagram illustrates a suggested workflow for redaction.



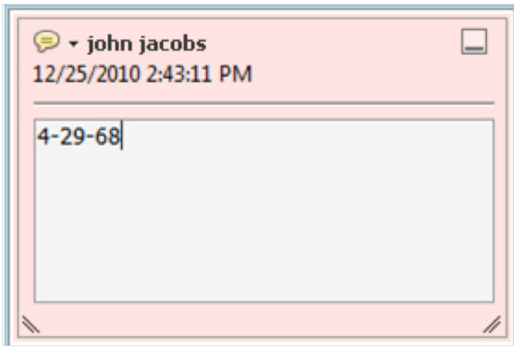
Example redaction workflow

Automatically copying redacted text to a sticky note

A redaction mark acts like a comment until you apply the redaction, which then permanently removes the information. A best practice is to set your preferences to automatically copy text into a sticky note, which are compiled in the Comments pane. Using sticky notes makes it easier to review, edit, and delete what is marked for redaction.

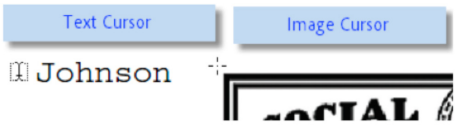
1. Choose **Edit** > **Preferences** (Windows) or **Acrobat** > **Preferences** (Mac).
2. In the Categories list, click **Commenting**.
3. Select **Copy Selected Text into Highlight**, **Crossout**, and **Underline Comment Pop-ups**.
4. Click OK.

When you select text using the Mark for Redaction tool, the text is automatically copied into a sticky note and placed in the Comments list.



Redacting text and graphics

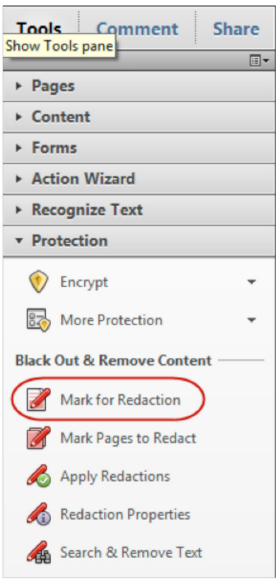
Use the Mark for Redaction tool to select text and graphics that will be removed from the document. The cursor changes depending on the type of content.



Note: Marking an item for redaction only flags the item for redaction. To finalize the redaction, you must apply it.

To select the redaction tool:

1. In the Tools panel, expand the Protection section.
2. Select **Mark for Redaction**.



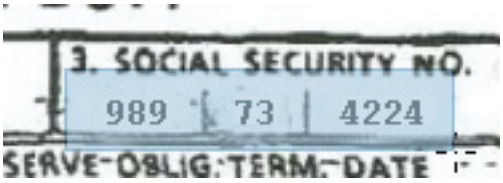
To redact text:

1. Select the **Mark for Redaction** tool.
2. Hover the cursor over the text that you want to redact. The cursor becomes a text selection cursor ( ).
3. Select the text to mark it for redaction.

> Tip: Did you select too much?
> Press Ctrl+Z (Windows) or Command+Z (Mac) to undo the redaction.

To redact a graphic or image:

1. Select the **Mark for Redaction** tool.
2. Hover the cursor over an image. When the crosshair cursor (+) appears, you can select the image.
3. Draw a rectangular selection around the area to redact. Everything within the selection area—images, text, and vector objects—is removed.

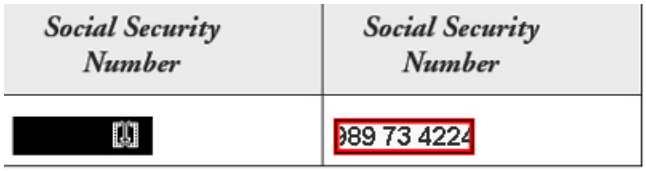


Still can't get a crosshair cursor?
Sometimes it is difficult to select an entire area that combines text and graphics. To get the crosshair cursor (+) for an area redaction, hold down the Alt (Windows) or Command (Mac) key.

Tip for redacting a photo
To select all the pixels in an image for redaction, double-click the image with the crosshair cursor (+).

To preview a redacted item:

1. Select the **Mark for Redaction** tool, if it is not already selected.
2. Hover over a redaction mark to preview it.



Preview with cursor over redacted object

Normal view shows redacted information

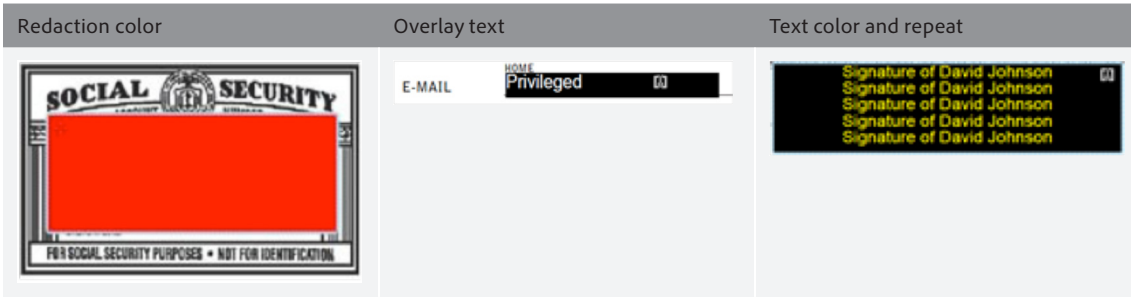
To delete a redaction mark:

1. With the Mark for Redaction tool, hover over the redaction mark and click to select it. You'll see subtle animation around the edges.

2. To delete the redaction, press the Delete key.

Changing the appearance of redactions

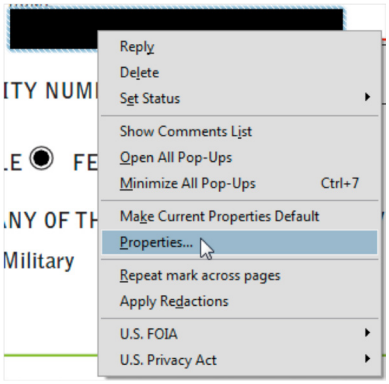
By default, redactions appear as solid black rectangles. You can change the appearance of redaction marks. For example, the image below shows different options.



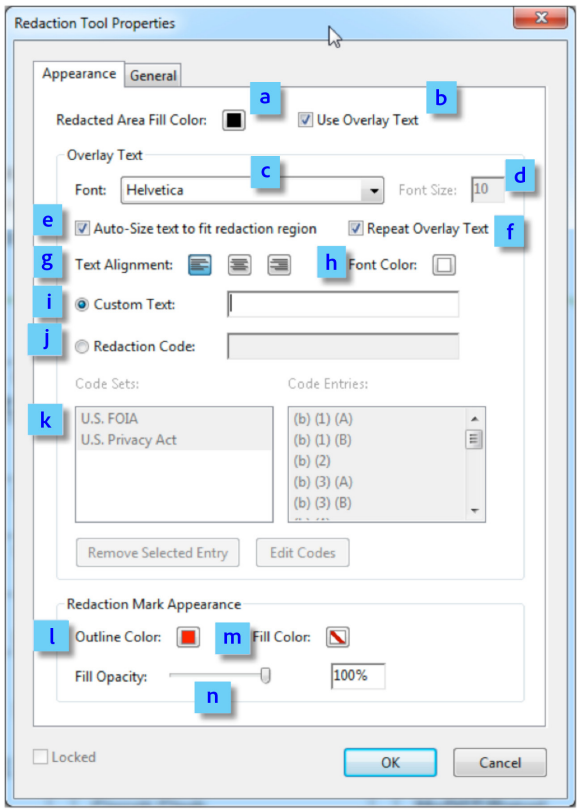
Examples of customizing the appearance of redactions

To change the appearance of a single redaction mark:

1. With the Mark for Redaction tool, hover over the redaction mark you want to change.
2. Right-click and choose **Properties**.



3. In the Redaction Properties window, select the changes that you want to make. The options are listed by letters in the screenshot below.



Redaction Tool Properties window

a. Choose the color of the redaction. You can also choose no color.
b. Select to have overlay text on top of the redaction.
c. Choose the font for the overlay text.
d. Set the font size for the overlay text.
e. Select Auto-Size Text to make the text fit the width of the redacted area.
f. Select to repeat the text over the redacted area.
g. Choose how to align the overlay text: left justified, centered, or right justified.
h. Specify the font color of the overlay text.
i. Select to enable custom text. Type the text to appear on top of the redaction.
j. Select to apply an exemption code. Exemption codes are listed in the box. You cannot change the information in this field.
k. Select a redaction code, if applicable. Redaction codes are pre-defined sets of text used to denote the reason or statute under which the redaction was made. Acrobat Pro includes two prepopulated sets— U.S. FOIA (Freedom of Information Act) and U.S. Privacy Act. You can also create and save your own sets.
l. Set the outline color for the redaction mark. This affects the appearance of the marked item only, not the final appearance of the redaction.
m. Set the fill color for the redaction mark. This affects the appearance of the marked item only, not the final appearance of the redaction.
n. Set the opacity of the redaction mark. This affects the appearance of the marked item only, not the final appearance of the redaction.

To change the default appearance of all redaction marks:

1. With the Mark for Redaction tool, select an item for redaction.
2. Right-click and choose **Properties**.
3. Specify the appearance of the redaction mark and click **OK**.
4. Right-click the redacted item and choose **Make Current Properties Default**.

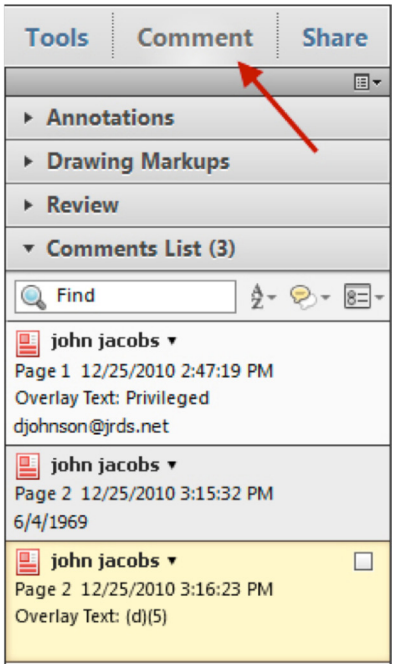
Frequently need to change the color of redaction marks?
Use the Properties bar instead. To open the Properties bar, press Ctrl+E (Windows) or Command+E (Mac). Select a redaction mark and change its color.

Deleting or changing multiple redaction marks simultaneously

The Acrobat Comments panel contains a list view of all redaction marks in the document. From there, you can delete or change the properties of multiple redaction marks at one time.

1. Click the Comment panel and expand the Comments List section.
2. Do one of the following:

- To select non-contiguous comments, hold down the Control key (Windows) or Command key (Mac) and click the comments you want to remove or change.
- To select all comments in the list or comments next to each other, select the first comment, and then while pressing the Shift key, select the last comment you want to remove or change.



3. To delete the comments, press the Delete key.
4. To change the properties of the selected comments, right-click and choose **Properties**.

Searching for text to redact

The Search and Remove Text feature allows you to search for single or multiple text strings and patterns, such as national ID numbers, within a single document or across multiple documents.

To search and redact text:

1. In the Tools panel, expand the Protection section.
2. Select **Search & Remove Text**.
3. For where to search, select the current document or browse to a folder of files to perform a cross-document search.
4. Select what you want to search for. If you choose **Multiple Words or Phrase**, the Words and Phrases to Search and Redact dialog box opens. Enter each word to search for and click **Add** or click **Import** to import a list of words.
5. Click **Search and Redact**. When the search is complete, the results appear.
6. To view where a result appears in the document, click the result.
7. Select the results you want to mark for redaction. To mark all the results, click **Check All**.
8. Click **Mark Checked Results for Redaction**.

Using pattern-based search

You can search for particular patterns to find information, such as phone numbers, national ID numbers, email addresses, and dates. To create custom patterns, see the section, "Creating custom redaction patterns."

To search for information using a pattern:

1. In the Tools panel, expand the Protection section.
2. Select **Search & Remove Text**.
3. For where to search, select the current document or browse to a folder of files to perform a cross-document search.
4. Under Search For, choose **Patterns**.
5. Select the pattern you want to find.
6. Click **Search and Redact**. The Search dialog box opens.
7. To perform a new search, click **New Search**.
8. To save the search to a PDF or CSV file, click the file icon.
9. To view where a result appears in the document, click the result.
10. Choose whether you want to mark whole or partial words. For partial word redaction, click **Settings**.
11. Select the results you want to mark for redaction. To mark all the results, click **Check All**.
12. Click **Mark Checked Results for Redaction**.

Reviewing redactions

It's important to review each page of your document, especially scanned documents. You can use the following familiar commenting and annotation Acrobat features to manage redactions:

- Add notes and comments to redacted items and send them to another Acrobat user to review, reply to, or change.
- Summarize comments and notes attached to redacted items as part of a review or archival workflow.
- Approve, reject, or delete items to be redacted using the Comments list.
- Participate in a Shared Review workflow, which allows you and your colleagues to use Acrobat X Pro to collaboratively redact documents.

To add a note or comment to an item marked for redaction, do one of the following:

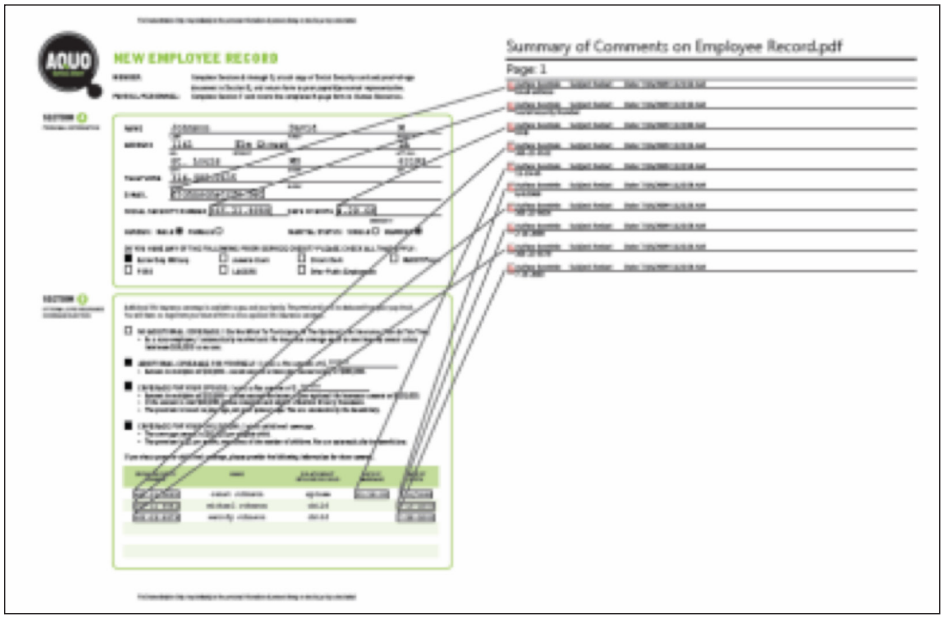
- Right-click the item and choose **Open Pop-up Note**.
- Double-click the item.

To view the Comment list:

- Click the Comments panel and expand the Comments List section.

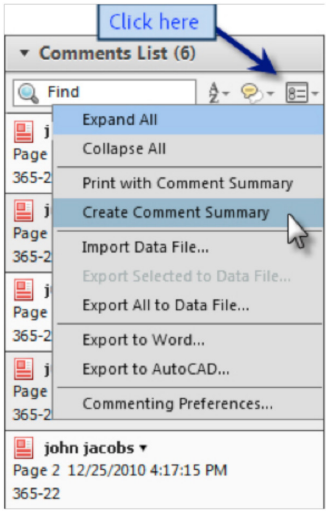
Creating a redaction summary

You can consolidate the comments of redacted documents in a single PDF file. Redaction annotations are displayed as callouts on the document.

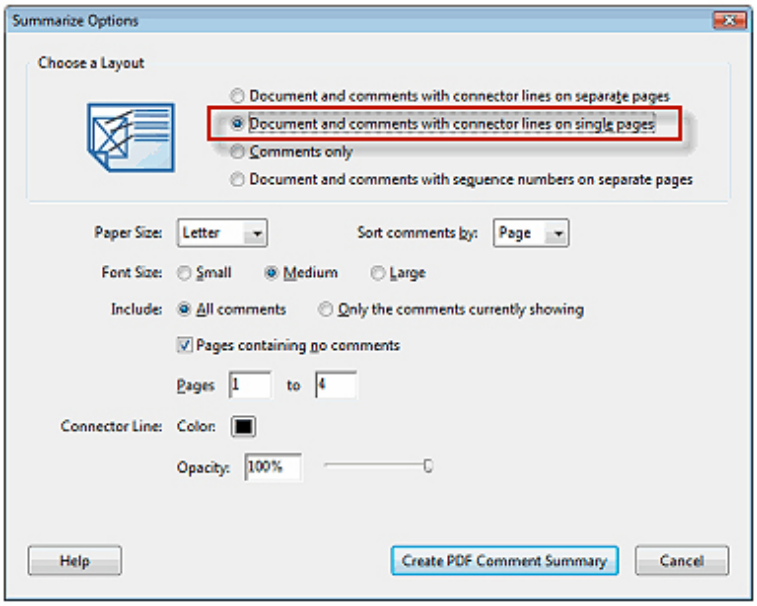


To create a summary:

1. Open the document containing your redaction marks. You must run this step before you apply the redactions.
2. Click the Comments panel and expand the Comments List section.
3. In the upper right corner of the Comments List, click the Options icon and choose **Create Comment Summary**.



4. In the Summarize Options dialog box, choose a layout option.



5. Click the **Create PDF Comment Summary** button.

Acrobat creates a PDF file that summarizes the redaction marks using the layout that you selected.

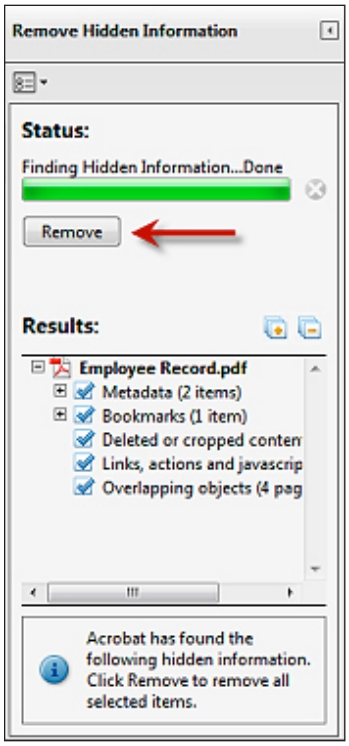
Applying redactions

You must apply a redaction to permanently remove the information from the document. All graphic objects such as text, raster images, or vector images that are fully covered by a redaction mark are completely removed from the document. All graphic objects that are partially covered by a redaction mark are modified so that only the covered area is removed. Any information associated with the graphic objects is also removed. After the redactions are applied, Acrobat prompts you to save the PDF document as a new file and will only include valid objects. This method prevents removed objects from being viewed or recovered in the future.

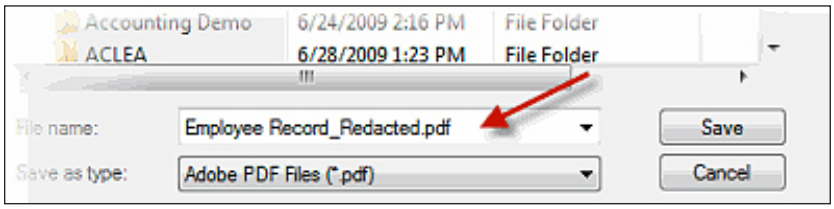
To apply redactions:

1. In the Tools panel, expand the Protection section.
2. Select **Apply Redactions**.
3. In the warning window, click **OK** if you want to remove the information.
   The redactions are applied.
4. In the message prompting you to examine the document for additional information, click **Yes**. This action finds hidden information, such as metadata, text, and comments, that could lead to an accidental disclosure.

5. Review the results and then click **Remove**.



6. Choose File > Save. Acrobat renames your file automatically when you save it.

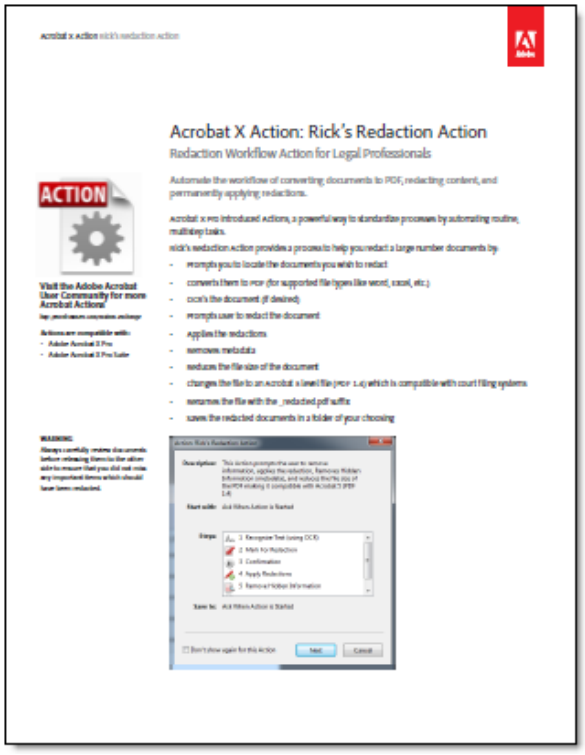


Automating Redaction Workflows Using Actions

You can use guided Actions in Acrobat X to automate many of the steps in the redaction process. With guided Actions, users are automatically taken through each step and prompted as appropriate, ensuring process consistency and minimizing the user's learning curve for Acrobat. For example, you can have an Action that performs the following steps:

1. Prompts you to locate the documents to redact.
2. Converts them to PDF (for supported file types like Word or Excel).
3. Performs OCR on the document, if needed.
4. Prompts you to redact the document.
5. Applies the redactions.
6. Removes hidden information and metadata.
7. Reduces the file size of the document.
8. Changes the file to an Acrobat 5 level file (PDF 1.4), which is compatible with court filing systems.
9. Renames the file with the _redacted.pdf suffix.
10. Saves the redacted documents in a folder of your choosing.

Download the above example action along with instructions (Redaction_Action.pdf).



Redaction_Action.pdf (674K)

You will need Acrobat X Pro to run the Action.

PDF file includes:

- Installation information
- Embedded Action
- Instructions on how to use the Action
- Customizing information

Tips and tricks for advanced users

Creating custom redaction patterns

Acrobat uses regular expressions—often abbreviated as REGEX—to find patterns. A regular expression is a code pattern that describes the attributes of the text that you want to find. For instance, if you need to find uniquely patterned account numbers, you can use a REGEX to find the pattern and mark all account numbers across many documents. For example, for the pattern of three alphabetic characters followed by three digits, the REGEX is \D\D\D\d\d\d. This pattern would find ABC123, but not 123ABC or A12345.

Several third-party tools are available for building regular expressions. For example, RegexBuddy (www.regexbuddy.com) is a Windows-based application for creating and testing regular expressions. It also comes with a library of prebuilt expressions for various patterns, such as postal codes, national IDs, and VAT country codes.

After you have created and tested a regular expression, you can add it to Acrobat.

Acrobat pattern files

Acrobat stores redaction patterns in an XML file called SearchRedactPatterns.xml. You can edit the file in a text editor like Notepad (Windows) or TextEdit (Mac). Before making changes, make a copy of the file. You can use existing patterns as a template. Copy the text you want to modify and place it at the end of the file, and then make the changes to create a new pattern.

Tip: It's easier to edit the XML file in an application that understands tags, such as Adobe Dreamweaver® or Microsoft Word.

Creating a new pattern

To create a new pattern:

1. Quit Acrobat if it is open.
2. Find the search pattern file:
   - (Windows XP)
     \Documents and Settings\<username>\Application Data\Adobe\Acrobat\10.0\Preferences\Redaction\<locale>\ SearchRedactPatterns.xml
   - (Windows 7 and Vista)
     \Users\<username>\AppData\Roaming\Adobe\Acrobat\10.0\Preferences\Redaction\<locale>\SearchRedactPatterns.xml
   - (Mac Intel)
     /Users/<username>/Library/Preferences/Adobe/Acrobat/10.0/ Redaction/<locale>/SearchRedactPatterns.xml

   Can't see the file on Windows?
   1. In the Control Panel, choose **Folder Options**.
   2. Click the **View** tab.
   3. Double-click **Hidden Files and Folders**.
   4. Enable **Show hidden files and folders**.
3. Make a backup copy of the SearchRedactPatterns.xml file.
4. Open SearchRedactPatterns.xml in a text editor.

5. Locate a pattern to modify. This example uses Entry4.

```
<set name="Entry4">
<str name="displayName">
<val>Email Addresses</val>
</str>
<str name="regEx" translate="no">
<val>([a-zA-Z0-9_])([a-zA-Z0-9_\-\.])*@([a-zA-Z\-])+\.([a-zA-Z\.]+)</val>
</str>
<str name="examples">
<val>This pattern will search for email addresses.

For example:
John.Doe@acme.com
John_Doe_1234@acme.gov
j-doe@marketing.acme.net</val>
</str>
</set>
```

6. Copy the block of text and place it just before the last tag in the file: </asf>.
7. Edit the block.
   a. Give the block a unique entry number.
   b. Change the display name. This name appears in Acrobat.
   c. Edit the pattern.
   d. (Optional) Provide a description and examples. Although this is optional, it is helpful for other users.

```
<set name="Entry4"> step 7a
<str name="displayName">
<val>Email Addresses</val> step 7b
</str>
<str name="regEx" translate="no">
<val>([a-zA-Z0-9_])([a-zA-Z0-9_\-\.])*@([a-zA-Z\-
])+\.([a-zA-Z\.]+)</val> step 7c
</str>
<str name="examples">
<val>This pattern will search for email addresses.
                                                step 7d
For example:
John.Doe@acme.com
John_Doe_1234@acme.gov
j-doe@marketing.acme.net</val>
</str>
</set>
```

Careful! Do not delete any quotes (" ") or brackets (< >).
Only fill in between the opening <val> and closing <\val> tags.

For example, a new Entry 6 for Canadian Social Insurance numbers looks like this:

```
<set name="Entry6">
<str name="displayName">
<val>Canadian Social Insurance Number</val>
</str>
<str name="regEx" translate="no">
<val>(\b)((\d{3}(-|\s|\.|_)\d{3}(-|\s|\.|_)\d{3})|(\d{9}))(\b)</val>
</str>
<str name="examples">
<val>This pattern will search for 9-digit Canadian Social Insurance numbers, either consecutive or 3 digits plus 3 digits plus 3 digits (separated by punctuation marks).

For example:
123-456-789
123456789</val>
</str>
</set>
```

8. Save the file.
9. Restart Acrobat.
10. Choose View > Toolbars > Redaction and then click the Search and Redact button. The new pattern should be in the list.

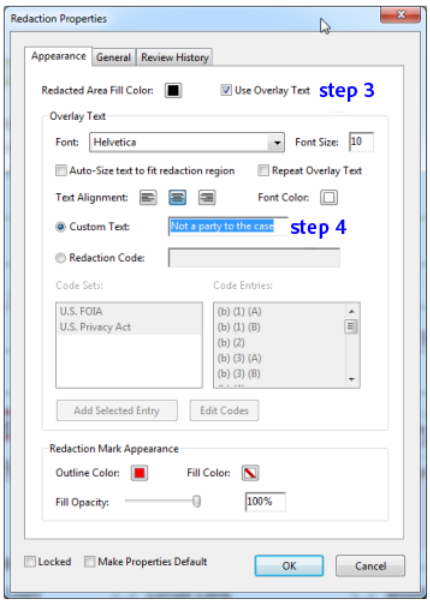
> **I edited the file, but the patterns aren't there!**
> Make sure that you edited the file in the Preferences folder.
> There is an identical file one level up that is easy to grab by mistake.

Adding overlay text and exemption codes to a redaction mark

Overlay text appears on top of a redaction mark and remains present after redactions are applied. The overlay text is useful for government agencies that are required to make documents public or to place a code or other mark on top of the redaction to meet agency guidelines.

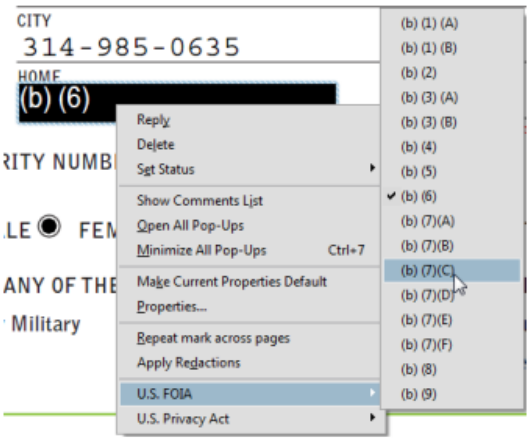
To add overlay text to a redaction mark:

1. Create a redaction mark.
2. Right-click the redaction mark and choose **Properties**.
3. Select Use **Overlay Text**.
4. In the **Custom Text** field, type the overlay text.
5. Click **OK**.



To add an exemption code to a redaction mark:

1. Create a redaction mark.
2. Right-click the redaction mark and choose the appropriate custom exemption code that appears in the menu and the appropriate code.
3. Repeat for as many exemption codes as needed per redaction.



Creating custom exemption code sets

You can create custom exemption codes to add to a redaction mark.

1. Create a redaction mark.
2. Right-click the redaction mark and choose **Properties**.
3. Click the **Edit Codes** button.
4. Click the **Add Set** button.
5. Change the name of the set in the entry field, and click the **Rename Set** button.
6. Click the **Add Code** button.
7. Change the name of the code in the entry field, and click the **Rename Code** button.
8. Repeat step 7 for as many codes as needed.
9. Click **OK** when you are finished.

Best practices summary

Keep in the mind the following when taking on projects that require redaction.

- **Do not forget to apply redactions!** Simply marking text and graphics does not actually remove it.
- Streamline the redaction process using Acrobat X Actions. You can use Actions to do the following:
  - Prompt users to manually redact pages
  - Perform Word List redaction
  - Apply redactions
- Carefully review scanned documents because OCR is not a foolproof process. The Search and Redact feature finds text only in searchable documents.
- Review all documents prior to submission. A two-person review team catches many more errors than a single person.
- Know your court rules and judge's orders regarding redaction. Ask the clerk of the court for clarification if you need more information.
- Don't skip the examine document step. Inexperienced users might only cover up information in electronic sources and mistakenly believe it is redacted. The Examine Document feature can detect and fix these issues.

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

91049010 5/11

Responding to personal data requests

Individual rights under the GDPR

One of the key objectives of the General Data Protection Regulation (GDPR) is to bolster the rights of individuals when it comes to their personal data. There are eight rights set out in the regulation, and we must process personal data in accordance with them.

They are:

1. The right to be informed about the collection and use of personal data, usually in a privacy notice.
2. The right of access to personal data - this is commonly referred to as a subject access request.
3. The right to have inaccurate personal data rectified, or completed if it is incomplete.
4. The right to have personal data erased – this is also known as the right to be forgotten and only applies in certain circumstances.
5. The right to request the restriction or suppression of personal data, which also only applies in certain circumstances.
6. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It only applies when your lawful basis for processing is consent or the performance of a contract and you are carrying out the processing by automated means.
7. The right to object to the processing of their personal data in certain circumstances, for example direct marketing purposes.
8. Rights in relation to automated decision making and profiling (i.e. automated processing of personal data to evaluate certain things about a person).

You can read more about these rights on the ICO website.

Dealing with a request

Members of the public might contact us about exercising the individual rights set out under the General Data Protection Regulation (GDPR). Requests do not have to specify the name of the right itself, or the relevant regulations.

You should familiarise yourself with what is involved so that you can recognise any request your business area receives.

Requests can be made in any format, although they are typically made in writing. They can only relate to the individual who makes the request, unless we have proof the requester (for example, a solicitor) is acting on behalf of the individual.

All requests must be fully responded to within 30 days, involve no charge for the requester, and any rejections should explain how an appeal can be made.

if you have any questions about data protection right requests contact the data protection and information assets team.

Note: This only applies to core Scottish Government. Requests relating to executive agencies should be referred to the data protection officer of the relevant executive agency.

Subject access requests (SAR)

Overview of subject access requests

People have a legal right to access the personal data held about them. They can make a subject access request (SAR) in writing, via an online form, by email or via official Scottish Government social media channels, along with proof of identification.

Organisations are no longer able to charge for subject access requests.

People might not refer to data protection legislation or use the phrase 'subject access request'. They may ask for example to see their file, copies of all their data, or ask what information is held on them. It should be treated as a valid SAR if it is clear that the person is asking for their own personal data.

A SAR should be passed immediately to the data protection and information asset team for core Scottish Government or the appropriate data protection representative within your executive agency.

Verbal requests

We also accept SARs verbally, for example in cases where the requestor is unable to make a written request due to a disability. In this case you should write down all the details and pass it to the data protection and information assets team as you would with any other request.

Requests made on behalf of other people

We can consider requests made by a third party on behalf of another person where we have the appropriate consent or power of attorney authority to do so. If you receive a request from a third party pass it on to the data protection and information asset team as soon as possible, who will then contact the third party to obtain consent or refuse the request where this cannot be obtained.

Responding to a request

We respond to a request as soon as possible, currently within one calendar month, as stated in the General Data Protection Regulation (down from the former limit of 40 days). All business areas must support requests and have a

process in place to supply the information to the data protection team (or executive agency data protection representative), in good time to allow a response to be finalised.

Further guidance

If you need help or advice email the data protection and information assets team.

Summary of the process - core SG

1. When a request is received you must send it to the data protection and information asset team (DPIAT) immediately who will advise next steps and the deadline for completing the response
2. The DPIAT will contact you, or the relevant business area to complete a search for the information requested. We will explain what action is required and provide an inventory to record any personal information identified
3. If you don't hold any personal data relating to the data subject let DPIAT know with a 'nil return' as soon as possible
4. If you do find personal data, carry out any redactions (blanking out exempt information) needed and prepare a copy of the documents for release
5. Complete an inventory of the documents included and the additional information questionnaire
6. Send the information, the questionnaire and the inventory to DPIAT before the deadline – mark it 'private and confidential'
7. DPIAT will reply to the requestor and keep a record of the request and copy of the inventory. The business area keeps hold of the documents and files correspondence relating to the request on eRDM (electronic record and document management system).

Role of the data protection team

The DPIAT is responsible for making sure that subject access requests are completed.

Their role is to:

- acknowledge and log the request
- check that the proof of identification has been requested and received

- where appropriate obtain consent or power of attorney for requests received from a third party acting on behalf of another person
- check there is enough information to identify the data requested
- contact the DG mailbox of the relevant business area with a search request
- send any paper documents securely to business areas
- provide data protection advice and guidance to business areas during SAR process
- issue a reminder email if the business area does not respond within the deadline
- receive the inventory form and the information in an appropriate format supplied by the business area
- return incomplete submissions to the business area if required
- check the data and any redactions
- when all the checks are complete, the team send the data to the requester in the appropriate format and close off the case

Searching for personal data

When responding to a subject access request you must do a full search of the business area's records. This includes personal devices, paper files, our electronic record and document management system (eRDM) and ministerial and corporate correspondence system (MACCS).

Personal data is anything which identifies, or can lead to the identification of, a living individual.

The search should be 'reasonable and proportionate'. This means the search should not involve a disproportionate amount of effort. Ask the data protection and information assets team (DPIAT) if you need advice on this.

Information should be current at the date it was released. You must not amend data held at the time of the request unless doing so is part of routine processing.

If you do not hold any personal data within the scope of the request, please confirm a 'nil return' to the DPIAT as soon as possible.

If the request is for personal images captured on CCTV we need to obtain sufficient details to allow us to identify the person, such as the date and time

of the recording and a description of the person. We also need to consider the nature and context of the footage and whether any other people need to be obscured (redacted) to protect their rights, if we are unable to get consent from them.

Providing the information to the Data Protection and Information Asset Team

If the request is made electronically, the information should be provided, where possible, in a commonly used electronic format.

Supplying a copy of CCTV footage

We are required to supply a hard copy of the footage unless the requestor agrees to view the content, or supplying it would involve disproportionate effort. A viewing should take place in a private place by appointment.

Large volume of information

Duplicate information across business areas is common but should still be submitted to DPIAT. If the search recovers a large number of documents, the requestor will be given the option to come in and view them rather than be sent them. They will also be asked if there are particular documents they are looking for or whether they want to see all of them.

Information relating to another individual

Subject access requests may involve providing information on another individual. Conflicts of interest might arise if the third party data is held alongside the applicant's data, for example a manager or colleague mentioned in an employee's file.

To make sure the third party's rights are not breached:

- if appropriate, ask the third party for their consent or check that it is reasonable in all circumstances to comply with the request without the consent of the third party
- use redaction using the same process as details requested under the Freedom of Information Act for individuals names and send what information you can.

If we do not have consent or we are not satisfied that it would be reasonable to disclose the third party information we should withhold it.

We are obliged to communicate as much information as we can so using redaction might be a better option.

Exemptions

People do not have the right to see their personal data where it is exempt from disclosure, under the provisions of data protection legislation.

Examples are personal data which:

- is subject to a duty of confidentiality, for example confidential references provided to the data controller
- is subject to legal professional privilege
- is being used to investigate crime or detect fraud
- is processed for the purposes of making Judicial, Crown or ministerial appointments

Exemptions are not mandatory and it is important to consult the data protection and information assets team for further advice in relation to exemptions if required.

If challenged, you must be prepared to defend your decision to apply an exemption to the Information Commissioner's office or the court. It is recommended that you keep a record of your decision.

Record keeping

The tables below explain the types of subject access request records which should be kept and for how long.

Business areas

Type of request	Description of record	Retention period
Standard	• correspondence about the request • inventory list	Two years from last action on case

	• copies of documents sent in response to the request – before and after any redactions	
Suspended	• correspondence about the request	Two months from last action on case

Data protection and information asset team

Type of request	Description of record	Retention period
All	• central listing of all requests	Permanent
Standard	• correspondence about the request • inventory list	Two years from last action on case
Suspended	• copies of correspondence about the request	Two months from last action on case

General Data Protection Regulation

7 things you should know

Definition of personal data: location data, IP addresses and online identifiers would constitute personal data in most cases as this data could be used to identify individuals.

Pseudonymization of personal data is considered a security measure used to limit the risk of singling out an individual.

Privacy by design (PbD) and privacy by default: must be used for systems development to ensure that privacy issues are addressed/built into systems in the initial stages of a project.

Broader scope: GDPR applies to both data controllers and data processors – it will impose direct obligations on data processors for the security of personal data and they can also be fined directly for non-compliance with GDPR

Data portability and right to be forgotten: allow individuals to request the dataset held by one organisation in a certain format so the individual can use it to pass to another organisation to process. GDPR also includes a right to request the erasure of personal data that is no longer necessary.

Accountability: review of what, why and how we process personal information and ensure that our documentation is fully up to date. This should include all privacy policies and ensure that these accurately reflect the purpose for which the data will be used

Data Protection Impact Assessments (DPIA): DPIA currently the Scottish Government policy, soon a legal requirement. The DPIA will allow to identify privacy risk at an early stage of any project involving personal data e.g. developing a new system

Data breaches and fines: It will be a legal requirement to report serious GDPR breach to the regulator, **within 72 hours**. There will be much larger fines for breaches of the Regulation up to 20 million euro.

Still not sure?
Contact us on:
dpa@gov.scot

This is not revolution, it's evolution

The new General Data Protection Regulation (GDPR) will come into effect from May 2018. As the UK will still be part of the European Union (EU) at that time the new law will apply to the UK while we still remain part of the EU. The GDPR will have a broad impact on the Scottish Government (SG). It will affect staff, systems, and information management and governance practices.

Digital Scotland

Data portability and subject access right

- Less time to comply
- The removal of the £10 subject access fee
- Subject access requests: revised guidance from the ICO
- Right to a copy of the personal data they have provided
- The format must be portable

Digital Scotland

What is changing ?

- Personal data – IP addresses, biometric and genetic data

- Accountability and transparency – contracts and privacy notices
- Data Protection Impact Assessments & Privacy by Design

- Data portability and right to erasure

- Logging and types of data subject (for data covered by LED)

- Data breaches and fines

- Data Protection Officer

safe

security action for everyone

General Data Protection Regulation

Subject Access Requests

6 Things You Need To Know About: Subject Access Requests

People have a legal right to access the personal data held about them. They can make a subject access request (SAR) in writing, via the online form, by email or via official Scottish Government (SG) social media channels along with proof of identification.

Here are six things you should know about subject access requests:

01 **A SAR should be passed immediately to the data protection and information assets team (for core SG only)**

02 **Individuals have the right to access their personal data and supplementary information**

03 **The right of access allows individuals to be aware of and verify the lawfulness of processing**

04 **A SAR should be made in writing**

05 **The £10 fee is being scrapped**

06 **The time for response has been decreased from 40 days to 1 calendar month**

Join the GDPR conversation. Go to the Data Protection Reform 2018 Yammer Group.
For guidance search for data protection on Saltire.

safe
security action for everyone

To report an incident, go to the Incident Reporting Tool on Saltire.

Extract from the Scottish Government data protection eLearning :

How should I handle personal data? (1 of 5)

The GDPR builds on an established framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to process personal data for business purposes with the rights of individuals in the protection of their personal data.

For the public, the GDPR gives people:

- the right to ask an organisation for all information it holds on them
- the right to be informed in writing whether personal data about them is held by the organisation and to have that information supplied to them
- the right to have their data updated promptly
- the right to ask the organisation to stop processing their data.

What are subject access requests (SARs)? (1 of 2)

Under the GDPR, the data subject has the right to find out what information is kept about them. The data controller (organisation) must respond within one calendar month. These requests are called subject access requests. In order for the organisation to respond to it, the request must:

- be in writing, many institutions offer standardised subject access request (SAR) forms as a letter, fax or email
- include the name and address of the data subject
- describe the information requested; if there is a need for further details to find the information, this can be asked of the person making the request
- come from the data subject (person), or their authorised representative, to whom it pertains once proof of identity has been confirmed.

If you receive a SAR it is worth bearing in mind that:

- no fee can be charged (unless under very specific circumstances) this is a change from the Data Protection Act where a £10 fee could be charged.
- all subject access requests (SARs) should be sent to the data protection & information assets team (DPIAT). The DPIAT acts as a liaison between business areas and data subjects.

How do we respond to a subject access request(SAR)? (2 of 2)

- As an organisation we cannot charge for subject access requests.
- The DPIA team verify the identity of the data subject (with assistance from the business when appropriate)
- If necessary, further clarification from the data subject can be asked for.
- The DPIA team inform the appropriate business areas of the request, once they are certain that the enquirer has the right to obtain the data. The SG then has one calendar month to respond to the request.

Some case studies (1 of 3)

Under the Freedom of Information (Scotland) Act 2002 (FOISA), a member of the public asks for all of the personal data held on people who attended a particular event at the Scottish Government. Should you disclose that information?

You should withhold it under the exemption at section 38(1)(b) (3rd party personal data) of FOISA. For more guidance see Step 3 of the Step-by-Step Guide to Handling FOI/EIRs Requests.

The eLearning finishes with a test, here are the questions about individual rights

Who can make a subject access request about a person?

- ○ **Anyone**
- ○ **Relatives of the person to whom the data pertains**
- ◉ **The individual to whom the data refers or their authorised representative**

20) How long do you have to respond to a subject access request (SAR)?

- [ ] **2 days**
- [x] **1 calendar month**
- [ ] **20 working days**

21) As an organisation how much can we charge for a subject access request (SAR)?

- [ ] **£10**
- [x] **No fee can be charged**
- [ ] **Up to £8**