WHITE PAPER

PROTECTING DATA WITH SECURE PDFS

HOW PDF FILES PROTECT YOUR DATA AND ENABLE SECURE AND COMPLIANT DOCUMENT WORKFLOWS

KOFAX

CONTENTS

INTRODUCTION

When documents fall into the wrong hands, or when their contents can be modified without authorization, it can mean serious and costly trouble for the business. Good news: the universal PDF format can be easily leveraged to mitigate these risks, with the right PDF solution.

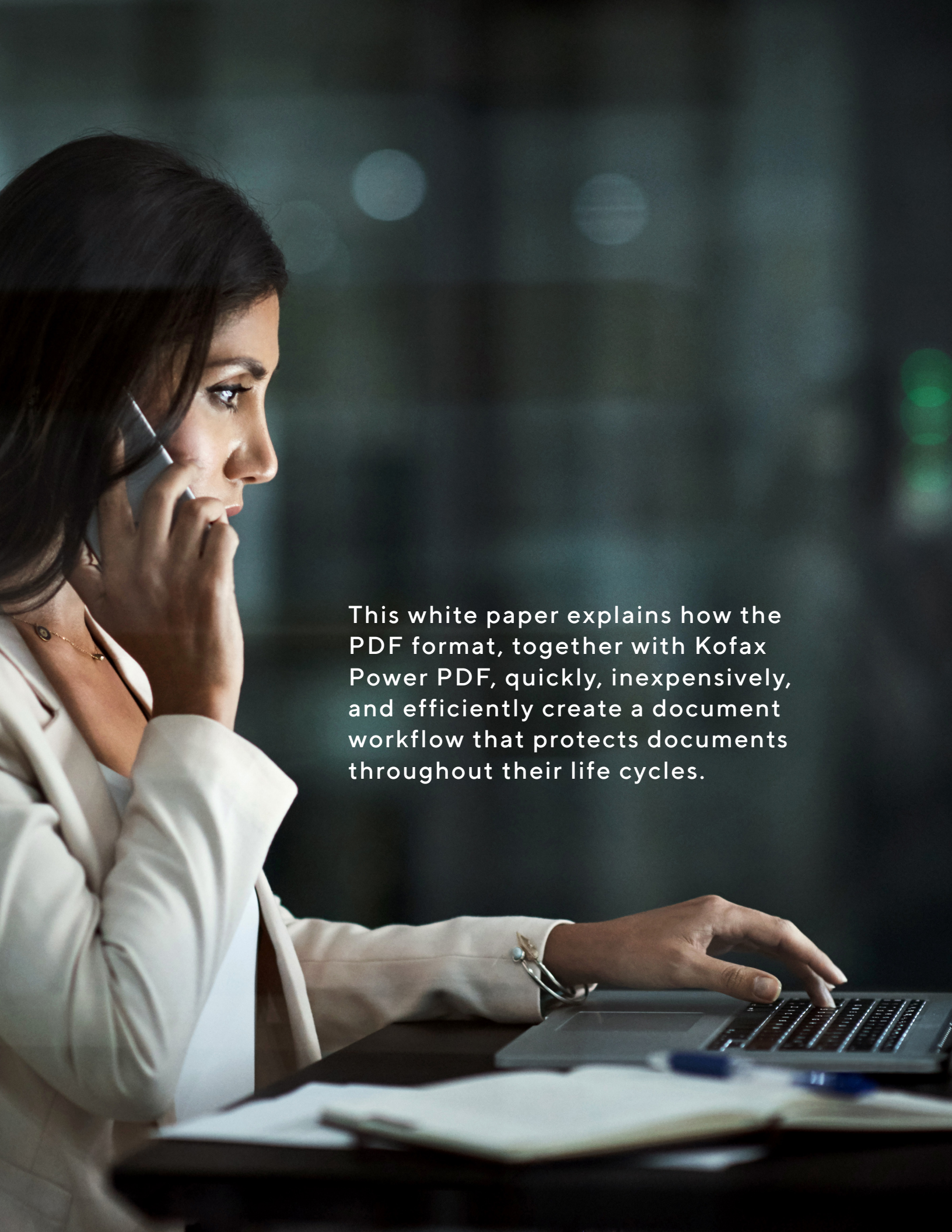
"P" IS FOR "PORTABLE"

The global average cost of a data breach now stands at $3.86 million, according to the 2018 study by Ponemon Institute. Are your documents the weakest link in the information security chain? Surely, no information source is so easily distributable: they're designed, in fact, for portability – so unlike the valuable bits and bytes in your fortress data centers. Yet, chances are, those portable documents are derived from the same potentially-sensitive information. But they're much less well protected.

PDF documents are designed for easy distribution—which is exactly why they're such a source of anguish to information security professionals. The same features that make PDF files such a productivity enhancer also expose the organization to serious security risks. An in-depth study of information security problems with Chief Information Security Officers (CISOs) sheds light on both sides of this challenging equation:

- 74% of CISOs have shared that employees in their organizations have expressed frustration at traditional "educate and prohibit" approaches to security.
- 80% of CISOs believe employees see security as a barrier to innovation.
- 71% of CISOs are made to feel like the bad guy by employees – because they're the ones saying "no".

There's got to be a better way. Organizations need the agility and productivity enabled by PDF files, but also observe security and compliance imperatives. What's needed is a PDF solution that both enables its users with easy portability and workflow support and secures an organization's data. Professional PDF solutions can deliver end-to-end security with easy-to-use features such as multi-level password protection, encryption, and configurable user permissions.



This white paper explains how the PDF format, together with Kofax Power PDF, quickly, inexpensively, and efficiently create a document workflow that protects documents throughout their life cycles.

DOCUMENTS: THE WEAKEST LINKS?

When documents fall into the wrong hands, or when their contents can be modified Your organization's employees are spending more time away from the office, and they're accessing documents from all over the world—often using their own, personal devices. Yes, "Bring Your Own Device" (BYOD) too often means "Bring Your Own Troubles."

This was demonstrated in a Ponemon Institute study of 2,300 IT specialists, finding that 58% of them consider BYOD a security risk. The use of private mobile devices restricts the effectiveness of data protection measures and impedes security policies.

It's all too easy for documents to fall into the wrong hands, or be accidentally or deliberately deleted, or even modified by unauthorized parties. And by "documents," we include patient information, financial details, customer drafts, contracts, personal contact information. When documents fall into the wrong hands it might not be just a temporary inconvenience, either. It can cause financial losses and potential penalties. HIPAA, PCI DSS, Sarbanes-Oxley—and the new giant, GDPR that stipulates penalties of €20M or 4% of total revenue (whichever is higher) for each breach.

And there are other costs. With faster distribution comes larger volumes of information, forcing organizations to increase physical or virtual storage space. This can drive added costs into five and six figures. And it isn't just infrastructure costs. The cost of protecting information against unauthorized access, whether from inside or outside the company, is also increasing.

PDF: FROM SECURITY LIABILITY TO ASSET

PDF is the most popular format for exchanging and archiving documents. Therefore, it's often viewed as one of the greatest potential risks. But with a complete PDF solution, that same portable data format can become a powerful tool for information security and can be surrounded with layers of protection.

PASSWORD PROTECTION: GOVERN WHO CAN VIEW AND EDIT PDFS

A powerful PDF solution configures access rights for PDF files, governing who can access, create, edit, save, print, and read each individual document. And the recently ratified PDF 2.0 file standard goes a step further by providing AES (Advanced Encryption Standard) revision 6 password support. It's like a website checker that shows whether the password you create is strong or weak. For added security, you're prompted to use special, non-Roman characters. You can set this capability individually, and for each separate document by using standard security profiles, or by assigning roles in global settings through Microsoft Active Directory Rights Management and other systems.

TWO ADDITIONAL PASSWORD SECURITY LEVELS INCLUDE:

1. Permission to open a document: If a document can only be opened with a password, it's protected against access by unauthorized persons, especially when combined with encryption.

2. Permission to edit a document: PDF doesn't just enable document exchange; it allows documents to be edited. Power PDF allow easy modification of texts, images, and formatting in PDF. But if a user wants to prevent this, he or she can use password security to determine:

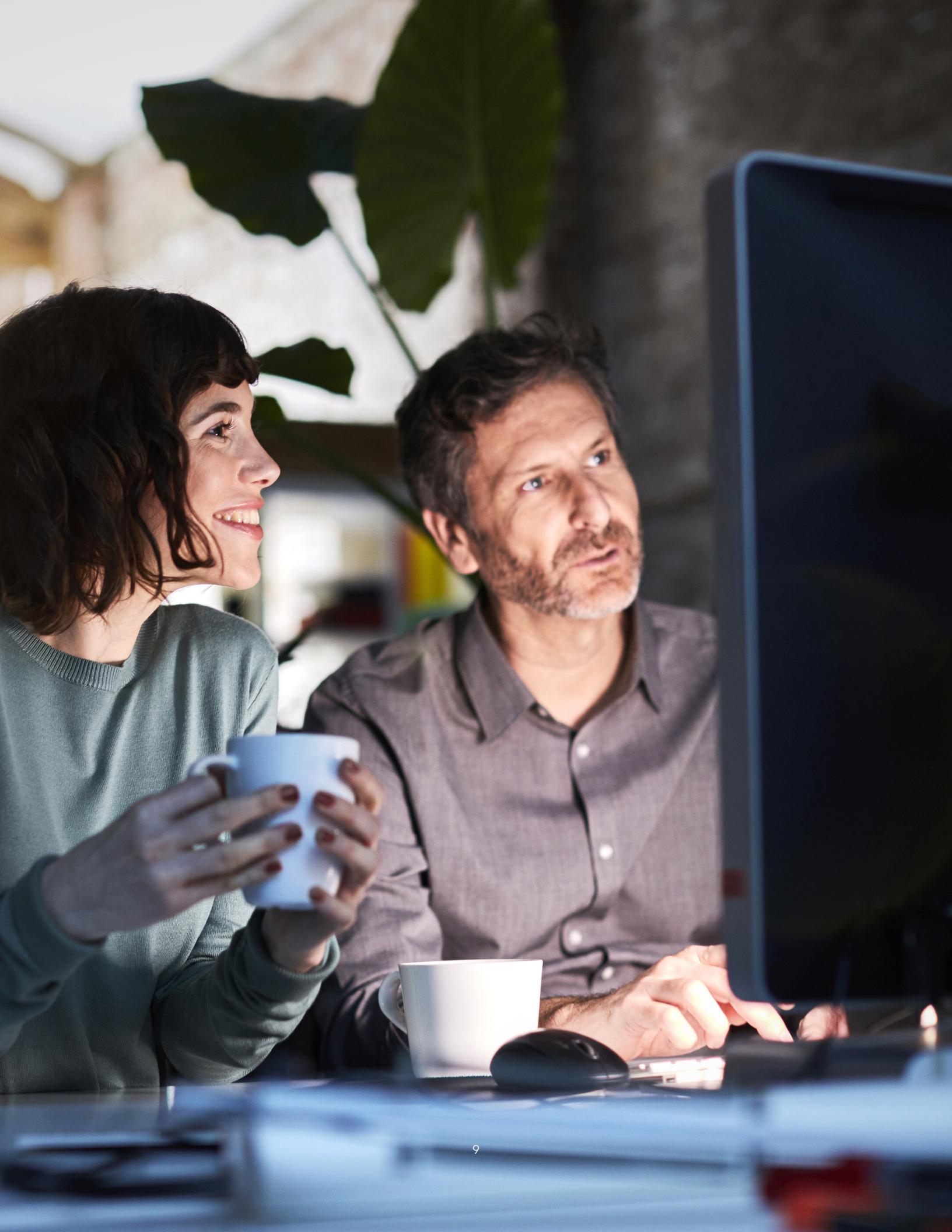
   - Whether or not a document may be printed, and which print resolution can be used
   - Whether or not pages may be removed, rotated, created, or added
   - Whether or not the recipient may fill in form fields and sign signature fields
   - Whether or not the recipient may add comments to the document

HERE ARE A FEW SNAPSHOTS OF HOW THIS CAN PLAY OUT IN REAL LIFE.

A project team leader can distribute a PDF file with confidential information via email without PGP or S-MIME encryption, using password protection to prevent any unintended party from viewing the document.

An employee who manages a project team can allow fellow team members to view, print, and add comments to a project plan—but not to remove or add any pages.

A customer can be allowed to complete form fields on an agreement and provide an e-signature, but not to change the text in any way.



IT'S ALL ABOUT THE TEAM: PLAYING NICE WITH DOCUMENT MANAGEMENT SYSTEMS

PDF documents can be seamlessly integrated with document management systems (DMS) such as iManage Work, Microsoft SharePoint, or OpenText eDocs through connectors that enable files to be opened directly within the DMS. External formats such as Microsoft Office, WordPerfect, images, or Microsoft's XPS documents can be converted directly into PDF format. And there's more:

- The user can select a single non-PDF file from the DMS interface and convert it directly into PDF in the DMS. The source files stay intact. The PDF takes the same name as the source and is normally stored in the same location as the original.
- Users can select a single non-PDF file from their computer, convert it to PDF, and save it in the current, or a defined, directory in the DMS system. In both cases, the conversions should be done without having to configure additional settings.

WORKING SEAMLESSLY WITHIN MICROSOFT OFFICE

When creating a PDF, Microsoft Office users should be able to define permissions directly from within the Office application. When saving a business letter, for example, an employee can specify that the recipient may print, but not edit, the document.

Business-ready PDF solutions allow users to add passwords directly to PDF files created in Microsoft Office, and prohibit or permit actions such as printing, extracting content, and editing. They can also assign different passwords to prevent documents from being opened and to specify different permission levels. When assigning permissions, predefined profiles can help protect typical application scenarios, such as forwarding a document to a business partner or team member.

UNDER LOCK & KEY: LEVERAGING ENCRYPTION ALGORITHMS

Encryption ensures that protected files really cannot be read by unauthorized persons. The PDF solution should support AES (Advanced Encryption Standard) with 256-bit key length: a standard, globally-used algorithm, specified by the American National Institute of Standards and Technology. The file should also be encrypted according to RSA standards in compliance with FIPS (Federal Information Processing Standard). The PDF 2.0 (ISO 32000-2) format now allows users to create documents with 256-bit AES revision 6.

Your PDF solution should offer backwards compatibility with older PDF applications, including:

- 40-bit RC4: Supported in PDF version 1.1 and above (security revision 2)
- 128-bit RC4: Supported in PDF version 1.4 and above (security revision 3)
- 128-bit AES: Supported in PDF version 1.6 and above (security revision 3)
- 256-bit AES: Supported in PDF version 1.7 and above (security revision 3)
- 256-bit AES: Supported in PDF version 2.0 and above (security revision 6)

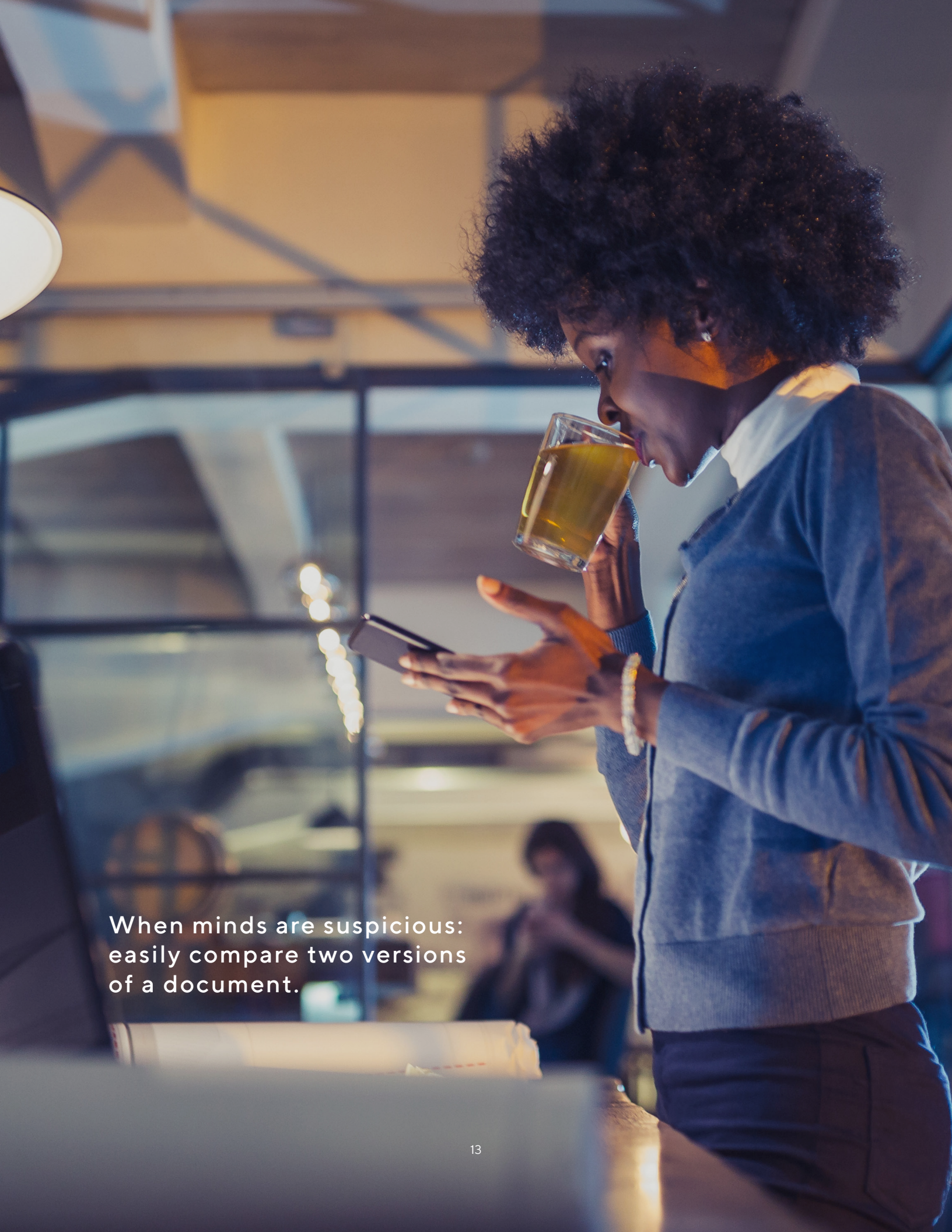
KEEPING IT ON THE DOWN-LOW: REDACTING CONFIDENTIAL INFORMATION

All companies handle personal information that is subject to data protection and can't be shared with third parties. This information includes: social security or credit card numbers, addresses, dates of birth, and medical information. Therefore, a PDF solution must be able to permanently remove this information in a traceable way. Potentially revealing metadata or other hidden information can be removed from the PDF as well.

When personal data must be redacted, however, it isn't enough to use the highlighting function to create a black line over sensitive information. Experienced PDF users can simply remove the added line, exposing the redacted content.

Instead, the PDF solution should remove the information permanently, while indicating that sensitive data has been removed from a specific location in the document.

It should also be possible to search, not just individual PDF files, but entire packages, portfolios, and directories, for information that needs to be redacted. A pattern search allows data in certain formats, such as credit card numbers or dates of birth, to be located accurately. Nevertheless, the user must always carefully check whether the document contains any searchable graphic elements that may also contain sensitive data.


When minds are suspicious:
easily compare two versions
of a document.

If there are any doubts as to whether a document has been modified or manipulated, a business-ready PDF solution will enable two document versions to be easily and quickly compared. In the process, it will clearly display any differences in the text, drawing objects, and graphics, as well as other information:

- **NUMBER OF WORDS THAT HAVE BEEN ADDED OR DELETED, AND THE NUMBER OF IDENTICAL WORDS**
- **NUMBER OF WORDS DIFFERING IN FORMATTING ONLY**
- **NUMBER OF IDENTICAL PAGES**
- **NUMBER OF DIFFERING PAGES**
- **NUMBER OF PAGES ADDED OR DELETED**

If the documents are not identical, the individual pages of both documents should be displayed side by side with differences highlighted. For example, deleted words should be crossed out, added words should be underlined, corresponding words surrounded by a box, differing graphics surrounded by a cloud, etc. For comparison purposes, blank pages must be added to the shorter document to equalize the numbers of pages.

FINAL SIGN OFF, WITHOUT THE HASSLE: E-SIGNATURE INTEGRATION

With proper integration, a PDF solution allows multiple parties to fully execute a contract in PDF form without the manual burden of printing, hand-signing, scanning,and redistributing the document. With DocuSign integration, e-signatures are accomplished with enhanced navigation that directs each party to sign or initial the document in the appropriate places, saving the file, and sending it to the correct party. Power PDF can create documents that are then signed, or sent for signature, in other leading e-signature services like Kofax SignDoc.

If unauthorized changes are made after a document has been signed, the digital signature becomes invalid. Documents may be signed several times and by different people. When selecting a PDF solution, ensure that it allows documents to be affixed with a digitally-authenticated time stamp. This indicates that the contents existed at a certain time and have survived without changes.

Digital IDs not only allow a PDF solution to authenticate documents, but to protect them. Known as certifying, this allows the owner of the document to apply a signature and document protection at the same time. The signee can completely lock the document or allow certain actions to be available for other users such as form filling or commenting. Users can use an existing digital ID or create their own. Each digital ID consists of a public and a private key. To enable others to verify the authenticity of a user's signature and document, they must be able to share their public key so they can then save their trusted identity store.

STILL NOT CONVINCED? HERE ARE 6 MORE GREAT REASONS TO USE KOFAX POWER PDF

1. **Easy configuration of read, edit, copy, and print authorizations.** Restrictions can be defined file-by-file for standard security profiles, or by assigning access rights via a Document Rights Management System. Power PDF Advanced also takes account of security settings that can be assigned in the FileOpen DRM system, as well as supporting Microsoft's Active Directory Rights Management Service (AD RMS), enabling administrators to define access rights within AD or Azure RMS and to apply them to PDF files. This works both directly using Power PDF and SharePoint workflows—and it doesn't require the document creator or the document viewer to take any special actions. No passwords needed.

2. **Strong encryption.** Power PDF uses industry-standard AES encryption, with a 128- or 256-bit key length. It supports the Public Key Cryptography Standard (PKCS) #12, while retaining backwards-compatibility to version 1.1 of the PDF standard. Word documents can also be protected directly when being saved as PDFs.

3. **Automatic or manual removal of sensitive data.** With Power PDF, sensitive data such as dates of birth, addresses, social security and credit card numbers are detected automatically when scanning paper documents and then redacted or removed. Hidden information such as metadata can also be removed automatically before sending a document.

4. **Digital signatures and certificates.** Documents can be signed and authenticated to guarantee their authenticity and integrity. Power PDF supports PKCS#7 and CAdES cryptography standards for signing and certifying documents, as well as DocuSign e-signature integration into the Power PDF user interface.

5. **Rapid implementation and integration with existing systems.** Power PDF generates of secure documents from office software such as Microsoft Office and integrates seamlessly into workflows in the latest Document Management Systems such as iManage Work, Microsoft SharePoint, or OpenText eDOCS.

6. **Compare two versions of a document.** Power PDF allows the user to view a comparison of different file versions, clearly displaying any differences between the versions.

CONCLUSION

PDF documents are designed for easy distribution—which is exactly why they're such a source of anguish to information security professionals. The same features that make PDF files such a productivity enhancer also expose the organization to serious security risks. Kofax Power PDF takes document security seriously, and is recognized by IT admins as a secure, low-hassle tool that their knowledge workers love to use. It delivers uncompromised value at a lower overall cost than any other PDF provider.

Allow us to answer your questions, or provide you with a demo or free trial of the software. See for yourself why thousands of customers have switched to Kofax Power PDF for their secure document collaboration needs.

For more information, visit KOFAX.COM/POWERPDF.

Work Like Tomorrow.™

KOFAX

kofax.com