WHITE PAPER

Using PDF Documents for More Secure Document Workflows

Secure creation, editing and archiving of documents.

KOFAX

Contents

Executive Summary

The management of extensive document sets is an inevitable reality for all companies. However, if documents fall into the wrong hands, either internally or externally, devastating problems arise. US companies face an average of $8.64 million per data breach, the highest average cost per country, according to the Ponemon Institute Cost of a Data Breach Report 2020. Complex regulations pertaining to such issues as breach notification are a major contributing factor to the higher US cost, especially since these regulations often vary from one state to another. Globally, the average total cost of a data breach is $3.86 million, with customers' personally identifiable information (PII) coming in as the most frequently compromised record type and the costliest. In addition to the financial risk involved, the company's reputation and loss of customer loyalty are also at stake when its internal information falls into the wrong hands. And if legal requirements are breached, the consequences for the company may be serious, potentially even leading to custodial sentences for senior managers.

Of course, safeguarding and keeping an eye on the many documents that a company creates, distributes, edits and stores throughout the document's entire life cycle is an extremely difficult task. Once paper documents have been circulated, it's virtually impossible to keep tabs on them. Managing documentation in digital processes based on the PDF format offers a far more successful alternative and is becoming the de facto standard in business.

Professional PDF solutions already feature security functions that can be combined with appropriate tools to create an end-to-end security workflow. For example, PDF supports optional password-protected document security with encryption and targeted allocation of user permissions using a separate owner's password.

This white paper explains how Kofax Power PDF can be used to quickly, inexpensively and efficiently create a document workflow that protects documents throughout their entire life cycle.

Documents: A security risk

It's becoming more and more difficult for companies to guarantee the security and integrity of their data, due in part to the increasing mobility of employees. Staff spend more time away from the office, accessing company documents from all over the world, often using their own devices. The "Bring your own device" (BYOD) trend poses a major problem for company security. Personal devices are typically more vulnerable to attack, as they are often older, or the user fails to install patches for known vulnerabilities and the most updated software versions. A recent report carried out by the Ponemon Institute discovered that 67% of IT professionals believe the use of BYOD devices during the pandemic has decreased their company's security posture. Another 71% are concerned that remote workers put their company at risk of a data breach[1]. The use of private mobile devices restricts the effectiveness of data protection measures and impedes the implementation of security policies. Increasing mobility and the use of cloud services to store and exchange data make it easier and faster to distribute and copy documents.

With mobility and the latest opportunities for communicating and reproducing information, the risk of data loss rises. When printed or distributed incorrectly, lists and documents can easily fall into the wrong hands or be accidentally or deliberately deleted by employees. If customer drafts, contracts or other confidential information are compromised, it's not simply a competitive disadvantage for the company concerned.

When data is lost or stolen, the company's competitive edge and reputation are at risk, and the organization may incur significant financial losses or be liable for heavy fines.

Regulations such as HIPAA, PCI DSS and SOX stipulate substantial fines or even prison sentences in the event of non-compliance.

Data is not only becoming more mobile. It's also distributed more quickly and created in larger volumes. The total amount of data created, captured and consumed in 2020 reached 59 zettabytes. This number is expected to increase rapidly every year, potentially reaching 149 zettabytes by 2024. One of the driving factors behind this massive increase in the volume of data is the push by companies in all industries towards digitizing information.

1. Cybersecurity in the Remote Work Era: A Global Risk Report

As organizations generate more data, they are forced to spend more on data storage. The global spend on data storage units is projected to surpass $78 billion in 2021. However, it's not just data storage costs that are huge; the cost of protecting such information against unauthorized access, whether from inside or outside the company, is also increasing. The consequences of data loss are becoming ever more serious, and this is clearly demonstrated by the aforementioned annual Cost of a Data Breach study performed by Ponemon. The report found that the average total cost incurred by companies worldwide due to a data breach has increased by 10% since 2014, rising from $3.5 million in 2014 to $3.86 million in 2020. The United States takes first place for the average total cost of a data breach ($8.64 million), followed by the Middle East ($6.52 million), Canada ($4.5 million), Germany ($4.45 million), Japan ($4.19 million) and France ($4.01 million).

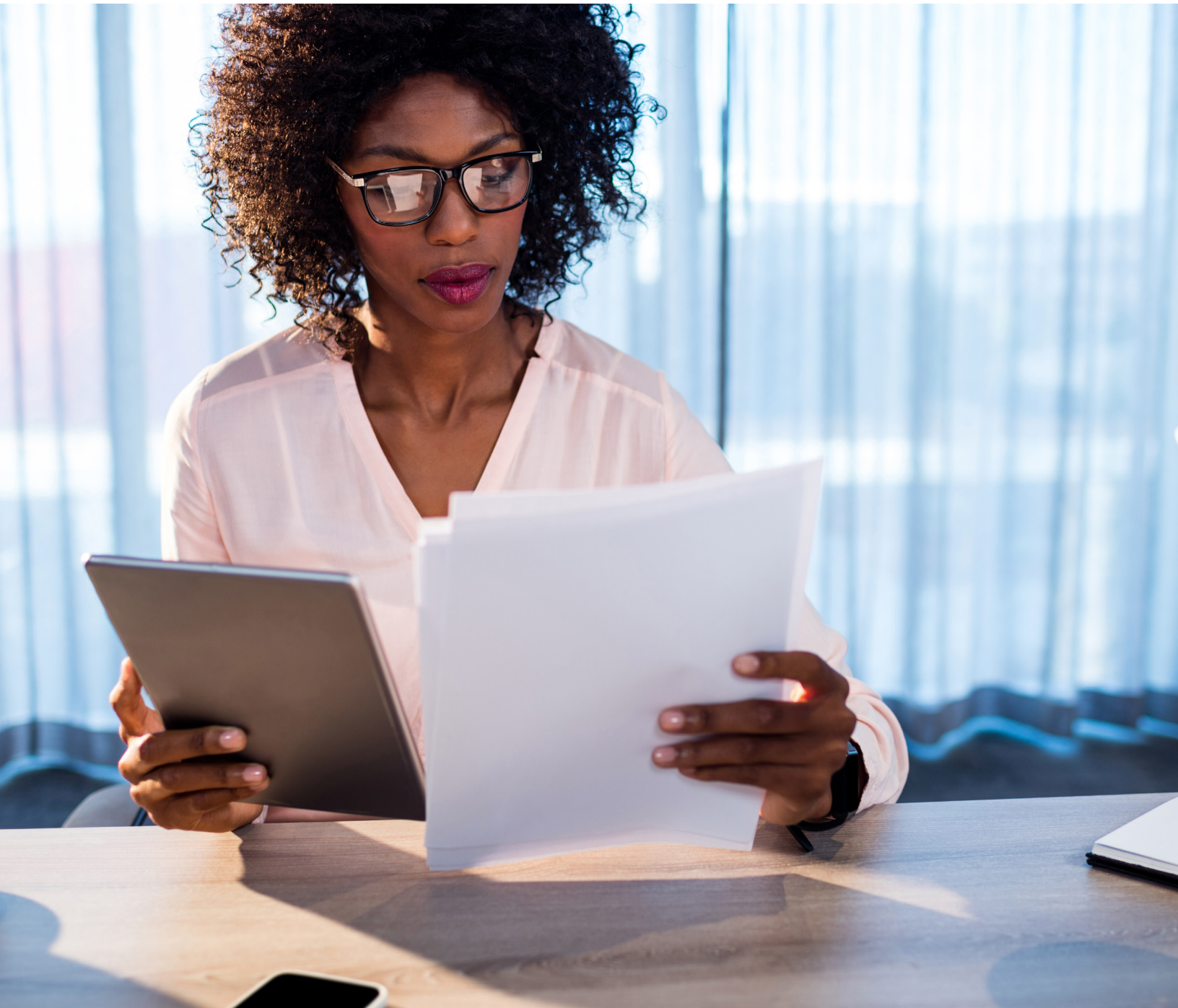
Companies operating in highly regulated industries also saw higher average data breach costs. The healthcare industry has the highest average cost ($7.13 million), followed by energy ($6.39 million), financial ($5.85 million), pharmaceuticals ($5.06 million) and technology ($5.04 million). The average per record cost came in at $149, with customer PII, intellectual property, anonymized customer data and employee PII among the most common types of compromised data. It's important to note the cost per record doesn't include the damage suffered through loss of reputation. According to Ponemon, the costs resulting from lost business account for nearly 40% of the average total cost of a data breach and increased from $1.42 million in 2019 to $1.52 million in 2020. When calculating the costs associated with lost business, Ponemon included customer turnover, lost revenue resulting from system downtime and the increased costs of winning new business due to a damaged reputation.

Companies—particularly IT teams—are well aware of the dangers of a breach. In fact, IT professionals are three times more concerned about the security of company financials and intellectual property than the security of their own home, according to the Oracle and KPMG Cloud Threat Report 2020.

It may be tempting to think that sticking with paper documents is the answer. However, paper documents are not necessarily more secure than electronic versions. In fact, quite the opposite is true. Once a paper document has left the printer, its journey from that point onward is difficult to control. It's impossible to know who might be able to read or copy it, and mishaps occur time and again during transport or disposal.

However, economic loss is only one of the serious consequences of a data breach. If companies are unable to prove that their data was protected according to the latest security standards, or that, in the event of loss or theft, no carelessness, negligence or even malicious intent was involved, they could face legal consequences.

If documents contain personal information, a number of regulations may apply depending on where business is being conducted and the industry involved. The General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS) are just some examples of the regulations with which your business may need to comply when it comes to data security and breach reporting. Several individual countries and states have issued their own set of regulations or plan to do so in the near future, making compliance an ever-changing environment that must be carefully navigated.



The role of PDF in secure document workflows

Even if, in principle, it's easier to keep digital documents under greater control than printed documents, digital formats still represent a potential security risk for companies. Therefore, document security is a central component of enterprise security, as the Ponemon Institute study demonstrates. Document security can contribute to maintaining data confidentiality, integrity, authenticity, accessibility, availability and usability.

PDF is the most popular format for exchanging and archiving documents. With a complete PDF solution, you can protect yourself by assigning security settings.

In particular, PDF documents can be protected at different levels:

Password protection: Restricted viewing and editing of PDF documents

The PDF solution should allow differentiated access authorizations to be defined for creating, editing, saving, printing and reading PDF documents. Ideally, it should be possible to set these functions both individually and for each separate document. For example, by entering passwords, via standard security profiles or by assigning roles in global settings via systems such as Microsoft Active Directory Rights Management.

In terms of password protection, you can choose between two levels:

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

Permission to edit a document: While PDF is initially only thought of as a way to exchange documents, this doesn't mean these documents cannot be modified. Professional solutions such as Power PDF allow easy modification of texts, images and formatting in PDF. Should you wish to prevent this, you must set a separate password to protect against editing. You can, for example, determine:

- Whether or not a document may be printed, and which print resolution to use.
- 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

Protecting the document against being opened is important if only a defined group of recipients is allowed to open it. For instance, if you send confidential information by email without PGP or S-MIME encryption, in principle, anyone who gains access to this email can also read the confidential document. But these tools can be costly.

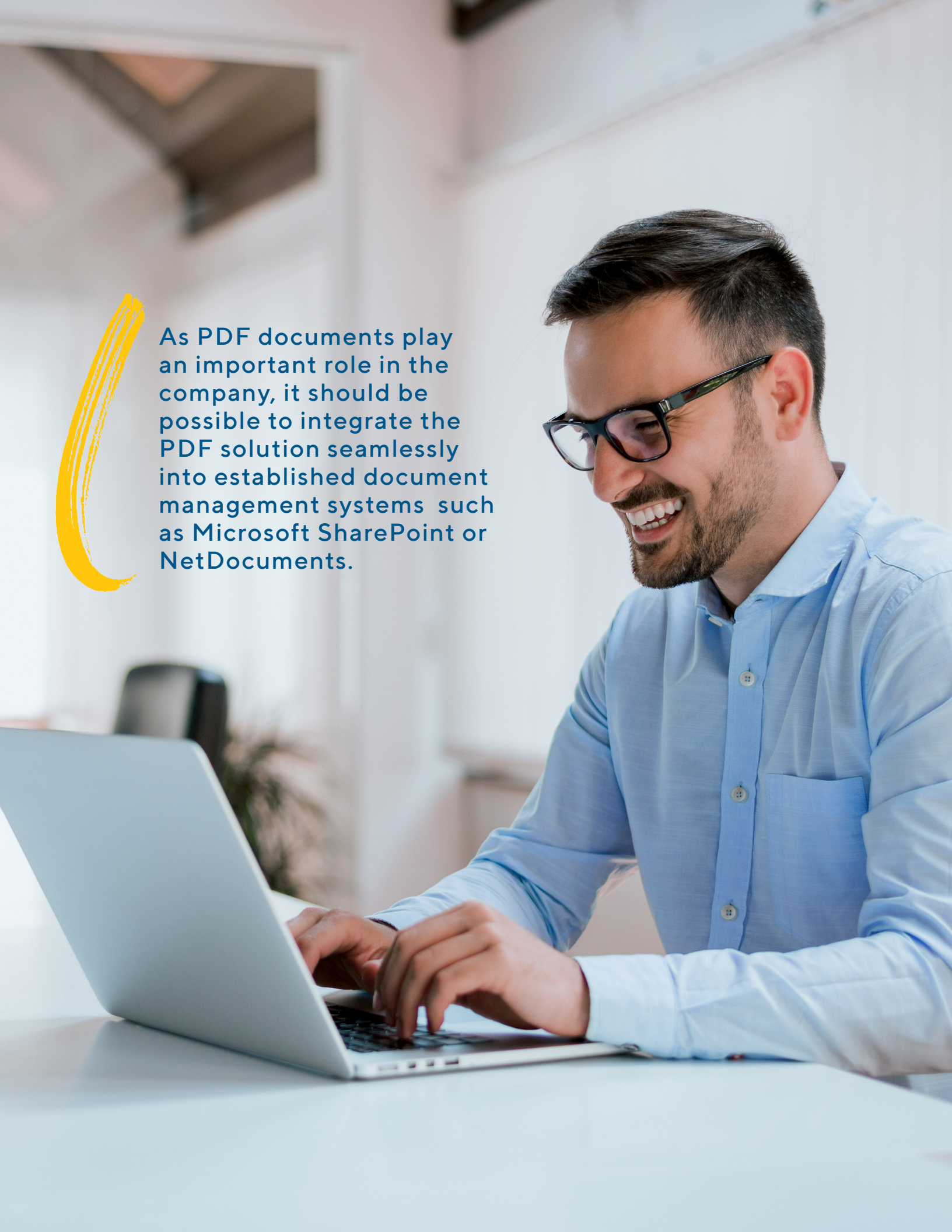
If the document is prevented from being opened or protected by a password, only the actual intended recipient to whom you have communicated the password (for example, by telephone or text message) will be able to open it.

Permissions passwords play an important role, above all when collaborating with internal or external co-workers, and also when communicating with customers. For example, if you manage a project team you might like the members of the team to view, print out and add comments to a project plan, but they shouldn't be allowed to remove or add any pages to it. Again, it should be possible for a customer to fill in form fields on an agreement and sign the document, but not to change the text in any way.

Integration with the Document Management System (DMS): Protecting access at the project or group level

Consistent document management processes avoid legal and financial risks for a company and provide a basis for proper accounting. However, these aren't the only advantages. Companies that classify, file and archive documents in a well-structured and orderly fashion also have a competitive advantage. For instance, a manufacturing company can keep track of product modifications far more easily, a graphic design studio can access and refine drafts at any time and a solicitor can call up the complete background to a case at the touch of a button. Teamwork is also greatly facilitated, as every team member can see who has created or edited a given document at any time. Versioning allows unwanted or rejected modifications to be cancelled, and different versions of a document to be tried out.

Integration is generally done using connectors that enable files to be opened directly from the Document Management System (DMS). During the process, it should be possible for external formats such as Microsoft Office, WordPerfect, images or Microsoft's XPS document format (XML Paper Specification) to be converted directly into PDF format, and for existing PDFs to be opened directly.



As PDF documents play an important role in the company, it should be possible to integrate the PDF solution seamlessly into established document management systems such as Microsoft SharePoint or NetDocuments.

Of course, PDF solutions should also operate in the opposite direction and enable documents to be checked into the DMS. It should be possible to integrate individual documents with the DMS and create PDF files directly outside of and within a DMS. The following options are possible:

- 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 local 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.

Protecting Microsoft Office documents when creating PDFs

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

The PDF solution should be able to add passwords directly to PDF files created in Microsoft Office, and prohibit or allow actions such as printing, extracting content and editing. Here too, it should be possible, as described above, to assign different passwords to prevent documents from being opened and to specify different permissions. When assigning permissions, predefined profiles can help protect typical application scenarios, such as forwarding a document to a business partner, team member or the public.

Encryption algorithm

To ensure that protected files really cannot be read by unauthorized persons, the files must be encrypted. During the process, the PDF solution should be able to support AES (Advanced Encryption Standard) with 256-bit key length, a worldwide acknowledged algorithm, specified by the American National Institute of Standards and Technology (NIST). The file should also be encrypted according to RSA standards in compliance with FIPS (Federal Information Processing Standard).

Even if the highest level of encryption is required, problems can still occur, as the encryption may not be recognized by older PDF applications. Therefore, the solution used should also be able to support older standards which may be less secure but are nevertheless more compatible with legacy software. Ideally, the user should be able to choose between:

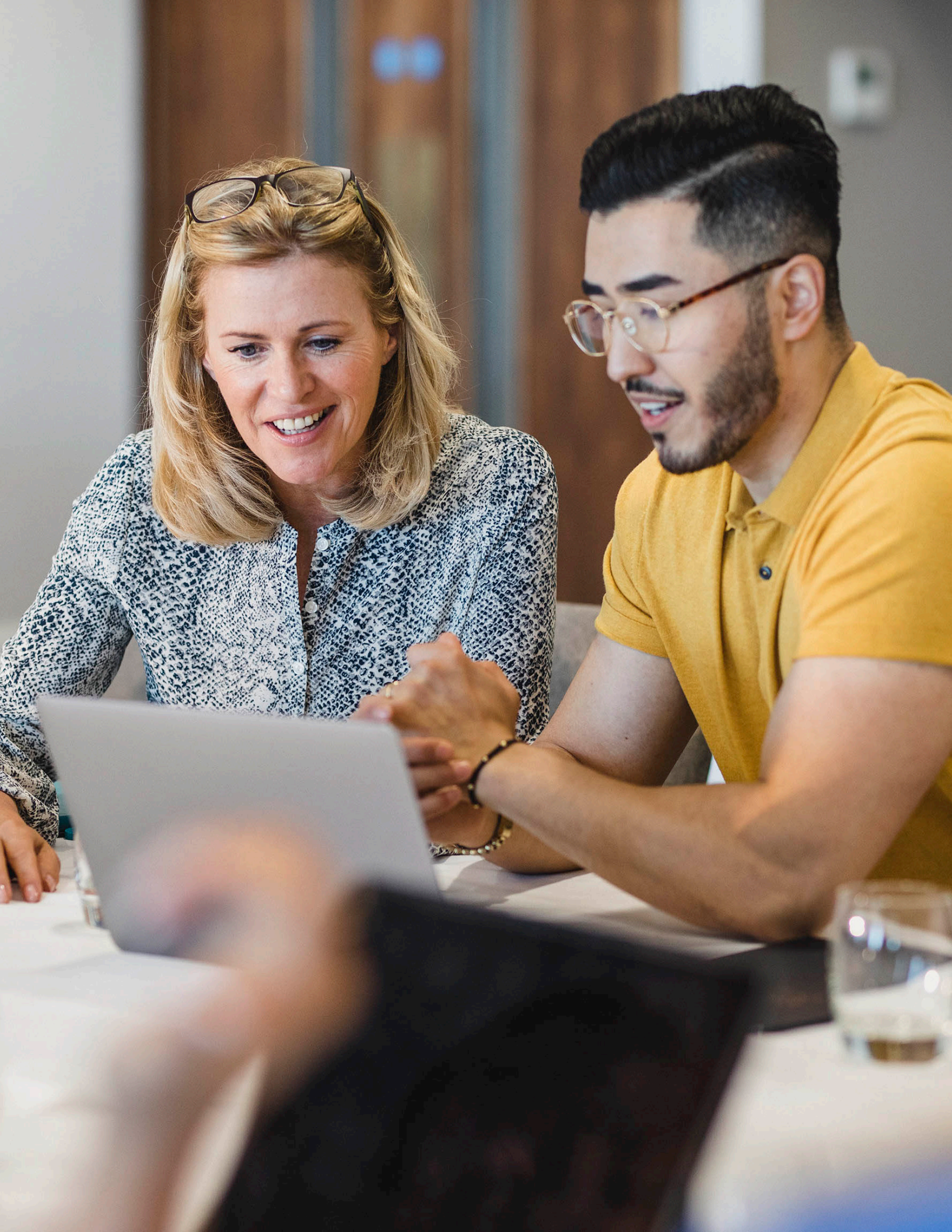
- 40-bit RC4 – Supported in PDF version 1.1 and above (security revision 2)
- 128-bit RC4 - Supported in PDF version 1.4 and above (security revision 3)
- 128-bit AES – Supported in PDF version 1.6 and above (security revision 3)
- 256-bit AES – Supported in PDF version 1.7 and above (security revision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

Permanent removal of confidential information from a PDF file

Personal data should be obliterated before the document is circulated in order to protect it. This process is often referred to as redacting. It's not enough to simply put a black line across the information that you wish to conceal, as an experienced PDF user would easily be able to remove this line again. Rather, the information must actually be removed permanently. Redacting the section in question simply indicates that sensitive data has been removed from this point in the document. This is particularly relevant for authorities and other public bodies, which are required by law to comply with information requirements and must inform the public of the fact that information has been removed from a document, specifying the section of text that has been removed.

All private companies have to handle personal information, which is subject to data protection regulations and must not be passed on to third parties. This may include Social Security or credit card numbers, addresses, dates of birth, religious affiliation, sexual orientation or political beliefs. Therefore, a PDF solution must be capable of permanently removing this information in a traceable way. This should be possible both manually and automatically. The program should also be able to remove potentially revealing meta data or hidden information from the PDF.

Ideally, it should be possible to search, not just individual PDF files, but also entire packages, portfolios and directories. A pattern search is also extremely helpful as it 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.

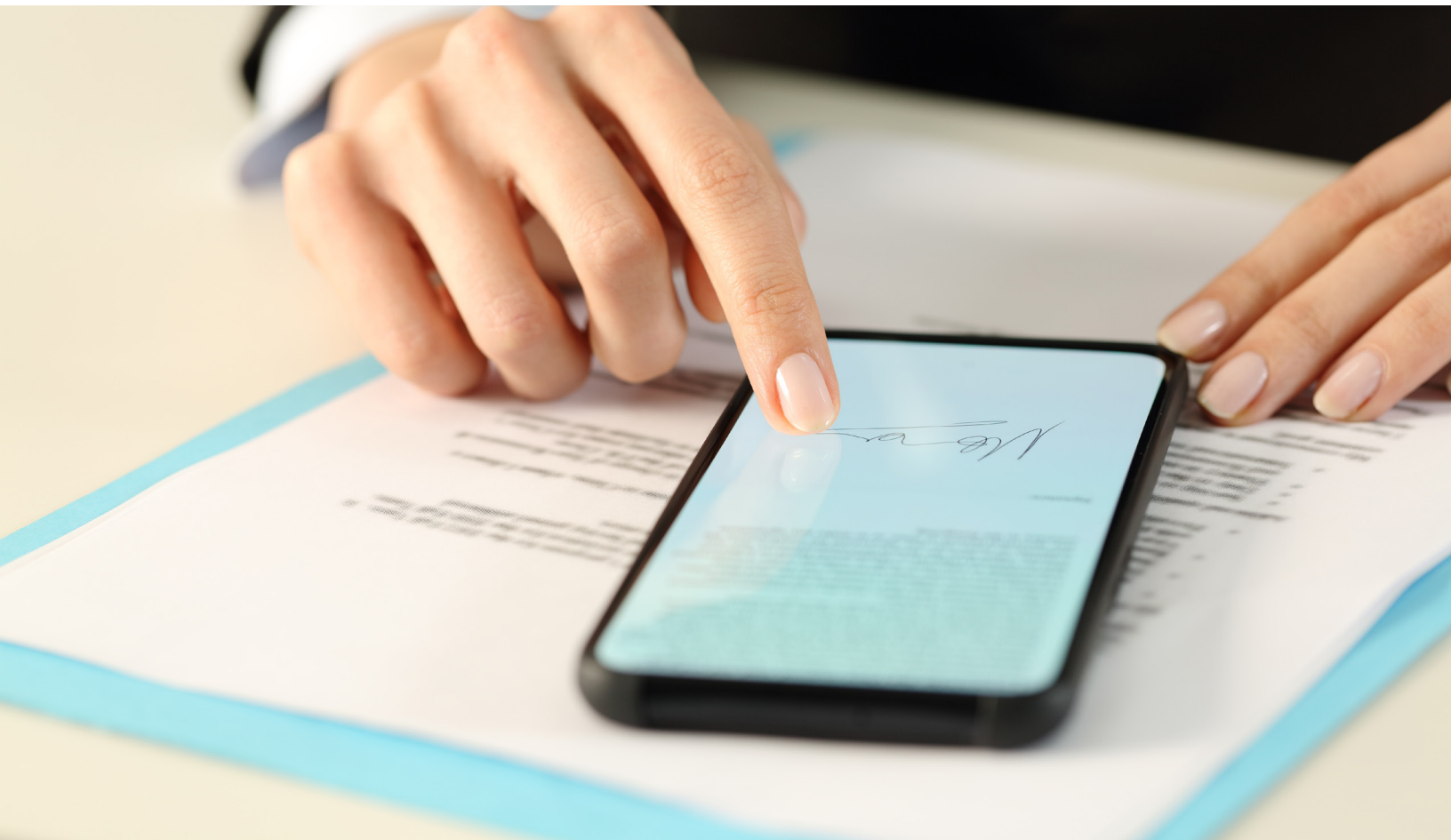


Comparing two versions of a document

Documents can be signed with a digital ID. This approximately corresponds to a signature on a paper document. If unauthorized changes are made to a document after it has been signed, the digital signature becomes invalid. Documents may be signed several times and by different persons. When deciding on a PDF solution, opt for an application that not only enables documents to be signed, but also allows them to be stamped with a digitally- authenticated time stamp. This indicates that the contents of any data file existed at a certain time and haven't been changed since that time. A time stamp is usually requested from a third-party along with a security certificate.

Digital IDs not only allow a PDF solution to authenticate documents, but also protects them. This process is known as certifying, and it 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. Organizations use this process to issue official documents.

For the purpose of creating the signature, you can either use an existing digital ID or you can create your own identity. Each digital ID consists of a public and a private key.
To enable others to verify the authenticity of your signature and your document, you need to share your public key with them, so that they can then save their trusted identities store.



Six great reasons to use Kofax Power PDF

Kofax Power PDF offers all security functions for creating, circulating and editing PDFs on a user-friendly operator interface. The main benefits of Power PDF in a secure digital workflow are:

1. **Easy configuration of read, edit, copy and print authorizations.** Restrictions can be defined on a file-by-file basis, for standard security profiles or by assigning personal access rights via a Document Rights Management System such as Microsoft Active Directory Rights Management. Power PDF Advanced also takes account of all security settings that can be assigned in the FileOpen DRM system. Only available in Power PDF Advanced: Microsoft's Active Directory Rights Management Service (AD RMS) is supported. This function enables administrators to define access rights via the Rights Management interface and to apply them to PDF files. This works both directly using Power PDF and in SharePoint workflows. It's an effective method of protecting your PDF documents against unauthorized access.
2. **Strong encryption.** Power PDF uses industry standard AES encryption, with a 128- or 256-bit key length and supports the Public Key Cryptography Standard (PKCS) #12, while retaining backwards-compatibility as far as 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 and Social Security and credit card numbers can be detected automatically when scanning paper documents and be redacted, partially redacted or entirely removed. Hidden information 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. Additionally, Power PDF uses technology that meets or exceeds FIPS requirements aimed at preventing fraudulent digital signatures.
5. **Rapid implementation and integration with existing systems.** Power PDF not only enables the generation of secure documents from office software such as Microsoft Office, but it can also be integrated seamlessly into workflows in such collaboration platforms as SharePoint, Google Docs, Box and Dropbox.
6. **Compare two versions of a document.** Power PDF allows the user to view a comparison of different file versions, clearly displaying any differences

Clearly, the cost of a data breach to an organization—financially, legally and reputationally—cannot be understated. With a complete PDF solution, you can protect your organization from negligence or malice and avoid potentially devastating consequences. Kofax Power PDF enables you to securely and efficiently keep your documents safe. So you can Work Like Tomorrow—today.

Work Like Tomorrow.™

KOFAX

kofax.com

August 20, 2021 11:20 AM