Are you ready for GDPR?

Best practices to implement a comprehensive document security strategy now.

In May 2018, the European Union (EU) will launch a new regulatory scheme for data protection that affects every business on a worldwide scale that markets to EU consumers.

As result, these organizations face new responsibilities—and potential liabilities—related to the way they manage business documents and related workflows.
Table of contents

3 Executive summary

3 What is GDPR, and why focus on it now?

4 Four key attributes of GDPR
   – Scope of data
   – Geographic impact
   – New mandates for businesses
   – Penalties for noncompliance

5 Preparing for GDPR

6 The focus on business documents

7 Six principles for managing business documents

8 Create a secure document infrastructure with Nuance solutions
   – MFP security
   – PDF security
   – Data loss prevention with OCR toolkits
   – Content screening
   – Print security, all the time
   – Secure mobile capture and access
   – Reporting

11 GDPR preparedness begins today with Nuance
Executive summary

In May 2018, the European Union (EU) will implement the General Data Protection Regulation (GDPR), a sweeping (260+ pages) replacement for a patchwork of national legal frameworks for the protection of personal data. More than four years in the making, the GDPR is intended to strengthen and unify data protection for individuals within the EU.

Failure to comply with GDPR can have severe financial consequences. Any organization that has a presence in the EU or the UK could face a fine of €20M or four percent of total revenue (whichever is higher) for each breach. Even those companies without a EU presence aren’t safe. U.S. laws now allow EU countries to create class-action lawsuits against U.S. companies, which may have to be defended in each country. Additionally, 29 U.S. states now have similar laws and can impose fines within 30 days of a breach where personally identifiable information (PII) is lost or exposed.

Unfortunately, there’s no clear path for how to achieve GDPR compliance, and without one, most companies find they have more questions than answers. In the scramble, most organizations start with general cybersecurity protocols, or addressing various vulnerabilities in infrastructure, platforms or applications. Yet in doing so, they overlook one area that will have a significant impact on GDPR compliance: business documents.

With so much PII data residing in paper and PDF documents, organizations need better ways to manage them, which includes all processes related to capture, conversion, collaboration, storage and security. This white paper provides a detailed overview of GDPR and its implications for global businesses today. It also highlights how proven solutions from Nuance Communications can help any organization improve the way it managed their critical documents to achieve GDPR compliance.

What is GDPR, and why focus on it now?

On May 25, 2018, the EU’s General Data Protection Regulation will come into force, affecting every organization that handles the personal data of any EU citizen. With new obligations for handling data, securing information and increasing transparency between businesses and individuals whose data/personal information they possess, IT teams everywhere will need to start (if they haven’t already started) rethinking their security in fundamental ways.

The GDPR imposes new obligations on businesses – anywhere in the world – that collect personal information from individuals residing in the EU, or that use or process such personal information. In parallel, the GDPR gives European consumers new rights and control over their personal data, including the so-called “right to be forgotten.”
Four key attributes of GDPR

There are four key attributes of the new regulation that demand the attention of any business that falls under its jurisdiction: the scope of the data it covers, its geographic impact, the new requirements that businesses must meet in order to comply, and the penalties for noncompliance.

Scope of data
“Exhaustive” might best describe the types of information that are required to be protected under the GDPR. In addition to the usual topics – such as names, dates of birth, and government ID (comparable to U.S. Social Security numbers) – the GDPR’s definition of personal data also includes home addresses, IP and email addresses, computing devices’ identifiers, online financial information, medical records, and a wide assortment of user-generated data, including social media posts and personal images uploaded to any website.

In a nutshell, virtually all personal data pertaining to European citizens or residents is considered theirs to share, or not; and businesses – referred to as “data controllers” or “data processors” – are obliged to protect it.

Each consumer is protected by a lengthy list of provisions, including the right to:

- Be informed and have access to data collected about them
- Rectify incorrect data
- Restrict processing and portability of data from where it’s stored
- Erase personal data or allow it to be forgotten

Geographic impact
The geographic reach of the GDPR also deserves attention. Any company outside the European Union that is targeting consumers within the EU will be subject to the GDPR. Its protections extend far beyond those citizens of the 28 EU nations who reside within the EU. For example, 29 U.S. states now have similar laws and can impose fines within 30 days of a breach where personally identifiable information (PII) is lost or exposed.

Also protected are EU citizens who happen to reside anywhere else in the world, as well as the non-citizen residents of any EU nation, regardless of nationality. As European consumers increasingly communicate with businesses on other continents that collect, use, or process their personal data, the impact will be genuinely global.

New mandates for businesses
Highlights of the many new requirements that the GDPR makes of businesses are:

- **Consent:** Consent must be given before any personal information can be processed.

- **Data protection officer:** Companies with more than 250 employees must appoint a data protection officer.

- **Privacy impact assessments:** For “risky” processing of personal data, data controllers must conduct privacy impact assessments.

- **Documentation:** Data controllers and processors must document all of their processing, and make documentation available on request.

- **Data breach notification:** Within 72 hours of learning of a breach that affects personal data, companies must notify the relevant EU authority. In addition, consumers affected by a data breach must be notified.

“Twenty-nine U.S. states now have similar laws and can impose fines within 30 days of a breach where personally identifiable information (PII) is lost or exposed.”
Penalties for noncompliance
The penalties that the GDPR specifies for companies that are not in compliance are stiff. They escalate from a formal written warning, to regular periodic data-integrity audits (which involve giving an auditor access to sensitive or proprietary information), to fines of up to €20 million or four percent of a company’s worldwide revenue, whichever is greater.

More, GDPR imposes an obligation of all organizations to report certain types of personal data breaches to the relevant supervisory authority within 72 hours of the breach. If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, the organization must also inform those individuals without undue delay. Even those companies without a EU presence aren’t safe. U.S. laws now allow EU countries to create class-action lawsuits against them, which may have to be defended in each country. Finally, 29 U.S. states also have similar laws and can impose fines within 30 days of a breach where PII data is lost or exposed.

Preparing for GDPR
The GDPR has been described by one of its legislative sponsors as “a fierce European ‘yes’ to strong consumer rights,” and it will clearly have an impact on all businesses that target those consumers. Yet the question remains: How should businesses prepare?

A sound strategy will include taking an organization-wide view of data protection – one that includes the business needs and opportunities posed by personal data, as well security and technology concerns. More tactically, there are technology solutions that can help any organization meet the GDPR requirements for secure capture, processing, management and storage of personal data.

The GDPR is designed to protect residents of the EU from fraudulent use of their personal data, which is exponentially on the rise worldwide and in the UK. For example, nearly 113 million personal records have been stolen in the UK since 2013. To comply with GDPR, organizations must ensure their information systems are secure and that effective data protection systems are in place. Additionally, organizations are required to obtain consent to store information and promptly notify authorities if a data breach occurs. They must also give individuals the ability to request access to their information and have their information erased if they choose.

Complying with these requirements could be a daunting challenge for any company, if it targets consumers in any of the 28 countries that make up the European Union, or plans to. The challenge is compounded by the explosive growth in overall data creation (163 zettabytes of new data every year by 2025, according to IDC); by the scope of data that the GDPR considers personal, including online financial information, medical records, social-media posts and personal images; and by the sheer difficulty of discovering and tracking all of the personal data your organization currently holds.
How can businesses improve these processes to better protect data and remain in compliance? The GDPR has a number of specific mandates for how the personal data of EU residents is handled, and what that will require as organizations attempt to improve the way they manage any and all documents that may contain personal information. These new or expanded protections include:

- Easier access for individuals to their own personal data
- The right to rectify and remove data, including the so-called “right to be forgotten”
- Data portability – the individual’s right to transfer his/her personal data when changing service providers
- Clear consent from the individual – an “opt-in” approach – required in order to collect, store, and process personal data
- Access to more and clearer information about how personal data is processed
- Limits on the use of automated processing of data to make decisions, e.g., through profiling
- Stricter safeguards for the transfer of personal data outside the EU
- The right to notification if personal data is compromised

The focus on business documents

The GDPR expects that, in order to avoid stiff penalties for noncompliance, organizations that maintain personal data will adopt a broad security strategy that includes monitoring and preventive controls. But beyond securing their IT infrastructure and taking inventory of their hardware, many organizations do not clearly understand what personal data is stored where, and who has access to it.

Business documents are a logical place to focus, since they typically tend to store customer information and other sensitive data — which means they likely contain personal data protected by GDPR. These are documents that appear as paper or digital files, which can be stored in a wide assortment of portable drives, file cabinets, personal files, shared folders, and document-management systems.

As a result, gaining control of documents and the processes involved with the print, capture, storage and overall use of information is essential, especially with the increase of 49 percent in data breaches relating to document workflows.

A handful of GDPR rules have direct, and specific, impact on how organizations treat their business documents. Key considerations are:

Encryption and anonymization: Businesses need to implement “appropriate technical and organizational measures to ensure a level of security appropriate to the risk” of breach1. Encryption is given as a specific example of such a measure. If documents are made unintelligible to unauthorized readers, the obligation to notify data subjects (individuals) about a breach can be eliminated.

A rule of least privilege for data access: Under GDPR, data processing is only permitted for a limited and defined purpose. The most effective way to control this is by limiting access to personal data, ensuring that only the people who need the data are able to read and use it.

1 The European GDPR website, https://www.eugdpr.org/
No non-essential personal data: Similarly, the GDPR introduces the concept of “data minimization”: organizations should only store the personal data that is essential for processing. This is also an effective way to reduce organizational risk, by removing data that holds little or no value but remains your responsibility to secure.

Increased transparency: Companies holding personal data are required to act transparently, to authorities and data subjects (individuals) alike. On an ongoing basis, companies must report on and demonstrate compliance with GDPR. In the event of a breach, they must notify the supervisory authority within 72 hours. In addition, within one month of a request, they must allow individuals to review the data you hold on them, free of charge.

Six principles for managing business documents

These principles of the GDPR regulation not only apply to data stored electronically but also all information stored in hardcopy files and prints. The processing and management for documents and information containing personal data must adhere to these six principles of the regulation.

1. Lawful, fair and accountable: Any information used must only be processed in a manner that is within the law, follows fair and correct usage and has transparency and accountability for the use built in.

2. Limitation of purpose: Information collected and maintained must only be used for the purpose that consent was given for its usage.

3. Data minimization: Documents and information should be stored with the minimum number of copies of the data required for the consented process.

4. Data accuracy: Information stored and used within processes should be accurate and allow the data subject the right to rectification.

5. Storage limitations: Information should only be stored when consent is given and when required for legal or compliance purposes. It should be destroyed once consent or compliance requirements have passed.

6. Integrity and confidentiality: All of the processing, storage and review of the personal information needs to be undertaken with integrity and confidentiality and under the regulation this needs to be provable.

Many organizations do not clearly understand what personal information is stored where and who has access to it. Implementing technology solutions to improve document processing, transportation, use and storage will help to ensure that documents containing personal information are stored and transported using secure methods and that copies are kept to a minimum within the compliance of the regulation.

Now Nuance solutions help to control and track what each user can and can’t do at a device, which is a prerequisite for the monitoring of unauthorized access and being accountable as required by the GDPR.
Create a secure document infrastructure with Nuance solutions

Organizations need to be ready for individuals requesting access to their personal data. But is that possible without organizational awareness or control over personal data storage? After all, a staggering high amount of personal data is stored in paper documents today.

Nuance document imaging and capture solutions enable documentation to be captured in protected digital formats and stored into central repositories, allowing the organization to reduce the number of copies of a document that exist in the organization. Having documents in digital format ensures they are transported between users and offices in a secure, encrypted and protected method.

With Nuance document imaging solutions, documents are securely captured into business workflows and processed ensuring personal information is utilized in accordance with the consent given by the subject of the personal data.

The following are examples of how Nuance solutions can help any organization improve security related to business documents to better comply with GDPR.

MFP security
Multi-function printers (MFPs) represent a significant risk to personal data in many organizations and a potential liability when it comes to GDPR compliance. Yet because most MFPs are connected to the internet, they offer anonymous “off ramps” to the outside world that many criminals will try to take advantage of. Secure MFPs and data protection at these network junctures is critical.

Nuance document capture and workflow management solutions enable organizations to restrict access to these devices and control what users can or can’t do at each device, including tracking and reporting of each user’s activities. These solutions provide easy access to a compliant audit trail to monitor all input and output from devices. Nuance solutions also employ data encryption to secure documents throughout business processes and workflows to ensure personal data is protected every step of the way.

PDF security
Document management is an inevitable fact of life for all companies. However, if documents fall into the wrong hands, either internally or externally, it can lead to serious problems for the business. The PDF format provides a secure framework for the reliable management of document workflows – everything from PDF creation and editing to archiving and deletion.

- **Encryption**: Nuance Power PDF™ solutions encrypt PDF documents using industry-standard AES encryption with 128- or 256-bit key strength and also support the public key cryptography standard (PKCS) #12. Microsoft Word documents can also be protected when saved as PDFs.

- **Personal information redaction**: Nuance PDF solutions also support GDPR compliance by automating personal information redaction. Documents sent via email, printer and copier are closely monitored for personal data. When identified, personal data is automatically redacted to ensure the security of the document and the safety of the customer’s information.
– **Digital signatures and certificates**: Documents can be signed and authenticated to guarantee their authenticity and integrity. Power PDF supports PKCS#7 and AES cryptography standards for signing and certifying documents.

– **Support for Microsoft’s Active Directory Rights Management Service (AD RMS)**: 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 also in SharePoint workflows. It is an effective method of protecting PDF documents against unauthorized access.

**Data loss prevention with OCR toolkits**
Data loss prevention may be just one specific example of the many security issues IT wrestles with – other areas include firewall management, network security, mobile devices and more – yet it is a top priority. By adding optical character recognition to software applications using an OCR software development kit, software engineers gain powerful new capabilities in the areas of document classification, routing and processing automation – critical for data loss prevention protocols.

Nuance’s OCR technology helps provide document intelligence that makes the content much more contextually aware. Then, the organization can create specific business rules to route (or restrict routing) to the most appropriate workflows based on a document’s content. For example, financial services organizations can use OCR to search for such terms as “confidential,” “internal only” or “sensitive information,” and then create business rules to prevent any document containing those terms from being emailed or distributed.

**Content screening**
Sometimes the greatest exposure to GDPR non-compliance is offline when content is being shared between employees and partners. Nuance solutions improve security by screening documents sent via email, printer and copier to ensure no personal data is left exposed.

Documents are screened to validate the sender and recipient, and content is searched for keywords, phrases and patterns as well as attributes or barcodes. Documents deemed at risk are quarantined in real time for immediate protection, with notifications to the sender, supervisor and security to ensure any violations or exposures are addressed immediately.

**Print security, all the time**
Global businesses can protect their data and ensure compliance with security controls that allow only authorized staff to access specific devices, applications and resources. For example, secure Follow-You Printing functionality allows users to print from anywhere, anytime they prefer and then pick up the documents whenever they want. This eliminates the risk of private information being left at a printer.

**Secure mobile capture and access**
Mobile workers need to access critical documents, and employees need to be able to securely deliver documents back into business processes or content management systems without increasing business risk.
Nuance mobile capture solutions connect workers to their networked Home Directory, other shared folders, and even SharePoint, anywhere, while maintaining existing corporate security infrastructure and IT policies. This eliminates the need for unsecured storage devices or third-party, cloud-based storage services.

**Reporting**
Despite increased investments in security solutions and headcount, companies are still likely to experience some form of data breach. In fact, evidence suggests that the number of cyber-attacks will continue to climb and continue to pose significant risks to businesses and consumers.

If the worst does happen, organizations need effective auditing and reporting tools. These are vital to understand what records were affected and to meet GDPR’s 72-hour requirement to notify regulatory authorities as well as those consumers whose data might have been compromised. For example, any transaction at a printer or MFP can be logged, and actual documents that were printed or scanned can be archived for future investigation efforts.

**GDPR preparedness begins today with Nuance**

GDPR reiterates the importance of preventing security breaches; preventive security measures help organizations minimize the risk of attack and should be part of the design of any solution to the processing and management of personal information.

Gaining control of print and capture workflows ensures that not only are documents transmitted to locations that are approved and compliant with an organization’s processes under the regulation, but the use of the workflows is controlled with user permissions ensuring that only authorized users have the ability to process personal information.

Implementation requires one or more of the following Nuance solutions: Nuance Power PDF, OmniPage, Nuance Equitrac, Nuance SafeCom, Nuance Output Manager, Nuance AutoStore and/or Nuance eCopy. Implementation also requires specific document workflows and devices that utilize these Nuance applications or combinations of Nuance applications on your network.

---

**About Nuance Communications, Inc.**
Nuance Communications, Inc., is a leading provider of voice and language solutions for businesses and consumers around the world. Its technologies, applications and services make the user experience more compelling by transforming the way people interact with devices and systems. Every day, millions of users and thousands of businesses experience Nuance’s proven applications. For more information, please visit [www.nuance.com](http://www.nuance.com).

---

Copyright © 2018 Nuance Communications, Inc. All rights reserved. Nuance and the Nuance logo are trademarks and/or registered trademarks of Nuance Communications, Inc., or its affiliates in the United States and/or other countries. All other brand and product names are trademarks or registered trademarks of their respective companies.

NDL_444 FEB 2018