GDPR compliance: The importance of securing your print and capture environment

An overview of the General Data Protection Regulation, and what you can do to make sure your organisation complies with its requirements.
Introduction

Managing unstructured information and documents is key to General Data Protection Regulation (GDPR) compliance. The regulation sets a baseline for data protection that requires anyone processing the personal data of an individual that is in the European Union (EU) to follow the requirements documented in the GDPR. It applies globally to all organisations processing personal data about individuals in the EU. Personal data is any information relating to the individual, be it private, professional or related to his or her public life.

Why the GDPR, and why now?

The GDPR is designed to protect residents of the EU from fraudulent use of personal data, which is exponentially on the rise worldwide and in the UK — nearly 113 million personal records have been stolen in the UK since 2013. To comply with GDPR, organisations must ensure their information systems are secure. Data protection should be by design and by default. Organisations are required to obtain consent to store information and promptly notify authorities if a data breach occurs. Individuals must also be able to request access to their information and have their information erased.

It is no secret that business documents represent a security risk when it comes to personal data. More than 60 percent of customer information is stored in business documents, which means they likely contain personal data protected by GDPR. Getting control of documents and the processes involved with the print and capture of information is essential, especially with the increase of 49 percent in data breaches relating to document workflow.

With encryption considered by the GDPR to be only one of the components of a broad security strategy, organisations need to consider monitoring and preventive controls based upon the sensitivity of the personal data they have. Failure to have in place accountable and provable processes, procedures and protection for personal data can result in the failure of compliance and fines of up to four percent of the company’s global annual revenue as well as reputational impact, material and non-material compensations for damages.

The cornerstones of GDPR compliance

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, 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 store and used within processes should be accurate and allow the data subject the right to rectification.

5. **Storage limitation**: Information and document should only be store while consent is given and for the legal and compliance requirements. 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 confidentially and under the regulation this needs to be provable.
Many organisations do not clearly understand what personal information is stored where and who has access to it. Implementing solutions into the business to enable a secure document processing, transportation and storage approach will enable the organisation to guarantee that documents containing personal information are only stored and transported using secure methods and copies are kept to a minimum within the compliance of the regulation.

How often is paper left unattended at the printer device? How many copies exist of a document? Who has copied it? Who has printed it? All these questions can be managed by securing the printing device. Control and track what each user can and can’t do at a device. Follow-you print services protect the authorisation. This is a prerequisite for the monitoring of unauthorised access and being accountable as required by the GDPR.

Creating a secure document infrastructure with Nuance solutions

Organisations need to be ready for individuals requesting access to their personal data. But is that possible without organisational awareness or control over personal data storage? After all, a staggering 60 percent 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 organisation to reduce the number of copies of a document that exist in the organisation. Having documents in digital format ensures they are transported between users and offices in a secure, encrypted and protected method.

MFP security

Multi-function printers (MFPs) represent a significant risk to personal data in many organisations and a potential liability when it comes to GDPR compliance. 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. Data protection at these network junctures is critical.

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

Content screening

Sometimes the greatest exposure to GDPR non-compliance is offline when content is being shared between employees and partners. Nuance solutions support your efforts 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 as well as to search content 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.
Personal information redaction

Nuance 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. Redacted content is stored and logged for further monitoring and then sent to the appropriate parties in a secure encrypted workflow.

Support for your entire workflow

We know how critical data is to your organisation and that it is used throughout your systems and processes. That’s why Nuance solutions are designed to integrate seamlessly wherever and whenever protection is needed, from line of business applications to groupware and collaboration systems, file, fax and email services, and office and production printers. Nuance solutions even extend to personal devices to support mobile workforces.

GDPR preparedness begins today with Nuance

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

With Nuance document imaging solutions such as Nuance AutoStore and Nuance eCopy, documents are securely captured into business workflows and processed safeguarding personal information is utilised in accordance with the consent given by the subject of the personal data.

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

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

To find out more about Nuance print management solutions in your local language, please visit our websites:

ENGLISH | FRANÇAIS | DEUTSCH | NEDERLANDS | ESPANOL | ITALIANO

For immediate help with answers to your questions, phone us on:

United Kingdom & Ireland +44 1628 491 651
Germany, Austria & Switzerland +49 6441 671 38446
Nordic countries +44 7825 169 378

BeNeLux +31 36 54 694 25
South Western Europe +33 1 79 97 40 68
East & Central Europe +44 7825 169 378

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.