White Paper

GDPR Compliance & Document Management

Why the need for GDPR?

We live in a connected world where the collection and sharing of personal data has exploded exponentially. Companies routinely gather vast amounts of personal data which can be easily stored, copied, moved and in the worst-case scenario sold or stolen. For example, a 16GB USB memory stick (less than £10 at time of writing) can easily hold 10,000 customer records containing important personal data.

In the days when paper records ruled, the physicality of paper offered a degree of protection as did the problem of quickly locating the relevant information. The European Union recognises the benefits of a healthy digital economy but has created the General Data Protection Regulation (GDPR) legislation to protect everyone's "personal data" (see Summary Definitions at the end of this paper).

Why bother when Brexit is on the horizon?

GDPR will apply in the United Kingdom from 25 May 2018 until it leaves the European Union - See UK Information Commissioner's Office https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr

The UK Data Protection Bill will be the UK view of GDPR and will replace the UK Data Protection Act 1998 (DPA) when it enters the UK statue books post Brexit - https://ico.org.uk/for-organisations/data-protection-bill

In other words, the UK Data Protection Bill will ensure a new Data Protection Act which enacts the GDPR's requirements – therefore, Brexit will not change compliance requirements.

Where are we now?

Most businesses have been bombarded with GDPR information; mailers, seminar invites, articles, etc. - the list goes on. Plus, we've got the technology companies jumping on the bandwagon and offering a quick fix: "buy our IT solution and solve all your GDPR compliance problems". In reality GDPR is a business issue and not simply an IT problem – but a quick technology fix won't necessarily make your business GDPR compliant.

However, using appropriate technology can make your life an awful lot easier! During this whitepaper we'll consider the useful role that a document management system (DMS) can play with regards to GDPR compliance.

Where is your data?

Under GDPR, any data needs to be accessible, audited and provided on demand at any moment in time. Understanding where data is held and retrieving it in a timely fashion is vital. Should that same data be subject to a security breach, GDPR also states that you have 72 hours to report the incident and present what preventative steps and remediation plans are in place.

Simply put, managing and protecting data in its basic sense is a series of requests and actions, something that most business software platforms should provide. But what about all of the unstructured data in your business - the documents and data which aren't held in a logical structure

or database and tagged with meta-data? An example of this would be the ubiquitous shared drive and let's face it, 99% of companies have got one. The shared drive is typically full to the brim with unstructured data, poorly organised, probably no version control, questionable security and no audit trail.

Potentially even worse, are cloud storage solutions like Google Drive, DropBox, ShareFile etc. where individuals (internal and external employees/partners) are given access to files and folders at a given point in time but are these permissions ever reviewed or tightly controlled? In addition, many experts argue a data breach is much more likely to happen on a major SaaS (software as a service) platform due to the scale of rewards (i.e. if you're a group of organised hackers you'll direct your efforts towards a major platform with the reward of a bigger pot of gold).

How can a document management system help with GDPR compliance?

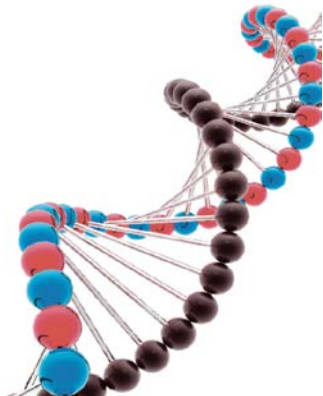
A document management system allows you to capture, manage and control documents (digital or paper) throughout an organisation. The key benefits are:

- Reduced Storage Space
- Enhanced Security
- Improved Regulatory Compliance
- Fast Retrieval
- Audit trail
- Better Collaboration
- Improved Backup and Disaster Recovery
- Workflow approval

Going back to GDPR, let's consider some key questions about how you currently manage documents:

- Can you quickly locate a document relating to a specific individual (e.g. a signed employment contract)?
- How long does it take to find it?
- Are there multiple copies of the same document and are you confident you are looking at the latest version?
- How confident are you that you've located the right document?
- Is access to the document restricted to those who really need to see or interact with it?
- Have you defined a retention and disposition policy?
- Do you have an audit trail showing who accessed a document, how did they interact with it and when?
- How easily could a document be copied, misplaced, deleted or even stolen?
- Is the document intrinsically safe – how vulnerable are you to a data breach?

A good DMS system will help with all of the above.



What are the key elements of GDPR and how does DMS help comply with them?

The right to be forgotten: The idea behind the right to be forgotten is to enable an individual to request the erasure or removal of personal data where there is no compelling reason for its continued processing. It is the responsibility of the data controller (see Summary Definitions) to delete and remove the data 'without undue delay' and specifically within a month unless specific circumstances apply.

Attempting to comply with the above can be a nightmare if you have a combination of paper records and digital files spread over multiple locations. If company policy is to store all important company records in a DMS then documents can be rapidly located using meta-data and quickly deleted if appropriate.

The right of access: The right for individuals to gain access to personal data that organisations hold about them is a key tenet of GDPR. This right entitles a data subject to ask a data controller:

- whether it processes their personal data
- what personal data they hold, the sources of such data, the purposes for which it is being processed and to whom it is disclosed
- To request copies of the personal data being held

If personal data is held in a DMS and tagged with relevant meta-data, it's a simple task to locate all the data held on a specific individual. As the information is held in a controlled environment you will know who has access to the data and you can even check who has interacted with the document/data over a period of time (via the audit trail). Even if data has been moved or deleted, you'll know by whom and when.

The right to data portability: Article 20 of GDPR allows an individual (Data Subjects) to request to receive their personal data, which they have provided to a Data Controller, in a structured, commonly used and machine-readable format (e.g. ASCII Text, CSV, XML, PDF), and to transmit it to another Data Controller. The aim of this right is to support user choice, user control and consumer empowerment. This can be very difficult to achieve if data is held in a variety of formats across multiple locations.

Using a DMS, data can be quickly located and exported in a variety of industry standard formats.

Breach notification standards: Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Whilst its clearly cavalier to argue the use of a DMS will stop data breaches, it certainly offers improved security through the use of access permissions and anonymisation of individual documents – data can also be encrypted at document, database or storage levels. It's also far easier to protect a single instance than many disparate silos of information (digital or paper). If a data breach does occur, a DMS can help identify the individuals involved and the data/documents effected.

Privacy by design: One of the changes due to be implemented under the new GDPR is the concept of 'privacy by design' and 'privacy by default'. Businesses must now consider data privacy at the initial design stages of a project as well as throughout the lifecycle of the relevant data processing. In simple terms, businesses should only process personal data where necessary for their intended purposes and should not store it for longer than is necessary for these purposes. In particular, the data controller should ensure that, by default, personal data is not made available without the individual's intervention to an indefinite number of people.

Using DMS retention and disposition polices it's fairly straight forward to decide how long data is held and when to delete it – without a DMS, this an onerous task. A DMS can also control who has access to the data, what level of interaction they have (e.g. list, view, copy, move, edit, delete etc.) and maintain an audit trail of who accessed information and when.

Summary Definitions

Data subject means an individual who is the subject of personal data.

Personal Data: According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

Example 1) opinions about the individual, or what is intended for them:

> A manager's assessment or opinion of an employee's performance during their initial probationary period will, if resulting information is to be entered into any computer based system, be personal data about that individual. Similarly, if a manager emails that an employee must do remedial training that will also be personal data.

Example 2) An organisation holds personal information in paper records:

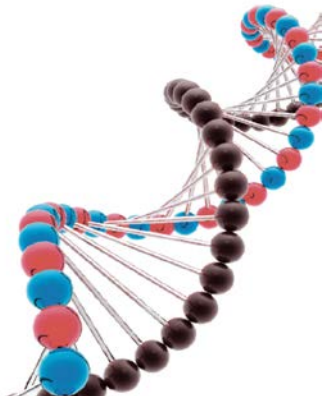
> Paper records which are held in an organised filing system structured either by reference to individuals or by criteria relating to individuals which allows ready access to specific information about a particular individual will be personal data.

(Personal data can even be when individuals are not identified by name, but bear unique reference numbers which can be matched to the individuals concerned. Plus, if it's possible that a person could be identified by a pseudonym, pseudonymised personal data can also fall under the law.)

Data controller means a person or entity who determines the purposes and manner in which any personal data is used, or will be used. (Term also applies when two or more persons or entities act together).

Any organisation (or individual) which has the authority to decide how personal data is to be processed is a data controller.

> Example: Any organisation with employees such as a Utilities company.



Data processor, in relation to personal data, means the person or group that processes (obtaining, recording, adapting or holding) the data on behalf of the data controller.

Data processors include accountants, payroll companies and call centres, all of which could hold or process personal information on behalf of someone else. "Cloud" service providers are usually data processors.

> Example 1) A utilities company engages a call centre company to provide its customer services functions. The call centre staff have access to the utility company's customer details but may only use the information they contain in accordance with strict contractual arrangements. The utilities company remains the data controller. The company that operates the call centre is a data processor.
>
> Example 2) An organisation employs a business services company to take care of its employee payroll. The organisation also engages a marketing company to carry out a customer satisfaction survey. The business services company will need information about the organisation's employees, and the marketing company will need information about its customers. Both companies will be processing the information on behalf of the organisation, and so they are both data processors. But, they will also be processing personal data regarding their own employees so will also be data controllers.

Data controllers & Data processors must ensure compliance to the new UK Data Protection Bill & GDPR. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Summary

This whitepaper isn't designed to provide a definitive guide to using DMS in regards to GDPR compliance, however we hope it has raised your awareness to some of the key issues involved and shown how DMS can help with a GDPR compliance initiative.

If you need more information on GDPR, the Information Commissioners Office (ICO) regularly publish information and offer helpful information on their website. If you need help or information regarding a DMS project please contact Document Genetics.

Author - © Joe Hyde, Sales & Marketing Director at Document Genetics

About

Joe Hyde is the Sales and Marketing Director at Document Genetics, an established UK based company providing a comprehensive range of business automation software. Document Genetics focus on improving document automation, workflow and collaboration within their client organisations, and their range of innovative solutions and specialist services help to save time and money by processing documents and data more efficiently. If you'd like to discuss your business process automation application with Document Genetics, we'd be delighted to help.

Hall Farm, Sywell Aerodrome, Sywell, Northampton NN6 0BN

t: 01604 671177
e: joe.hyde@document-genetics.co.uk
w: www.document-genetics.co.uk

DOCUMENT genetics
business automation software