Arena group the document experts

# GDPR: AN ESSENTIAL GUIDE

**General Data Protection Regulations or GDPR is legislation that relates to the use of an individual's personal data that impacts on ALL organisations and will fundamentally change how we should gather, use and store personal data.**

With the May 25th 2018 deadline looming, the risk of increased fines for breaches, and the need to change activities and processes we take for granted, now's the time to act.

This briefing by Arena's Neil Maude, provides a summary of the key changes expected in the upcoming EU General Data Protection Regulation.

Speak to our experts to find out more: **0344 863 8000**
info@arenagroup.net | www.arenagroup.net

New data protection regulations will come into force as of May 25th 2018. The UK government and Information Commissioners Office have confirmed that **Brexit will not affect the implementation** of GDPR legislation in the UK. Whilst EU-led, this is happening for UK organisations in 2018.

## What is GDPR?

General Data Protection Regulations or GDPR is legislation will come into force on May 25th 2018 that updates the existing Data Protection Act (1998). DPA1998 already provides an individual with rights of protection of their personal information, whilst GDPR increases some levels and removes constraints in other areas.

Although GDPR builds on DPA1998, a key concept is **accountability** – that organisations must be **responsible for, and able to demonstrate, compliance with the principles.** Those organisations must be able to show **how** they are taking appropriate care of personal data. Clearly, **"how"** is a broad term – it places an obligation on organisations to have documented procedures and be able to demonstrate that personal information will only be **processed lawfully** and will be held in an **appropriately secure** manner.

Further, organisations are expected to only collect information which is limited to that necessary for the purposes for which it is processed, that the information is accurate and is kept for the minimum period.

The penalties for breaches of GDPR are far higher than in the past – up to 4% of global turnover, or €20M, whichever the higher. It is not expected that the ICO will levy such fines immediately or in minor cases, but there is a much stronger motivation for organisations to protect themselves from this risk.

> Penalties for breaches of GDPR are far higher than in the past – up to 4% of global turnover

## What you need to know

Much of the GDPR legislation is a strengthening or updating of DPA1998, but the following are some of the main points that will be relevant to most organisations:

### 1 Subject Access Requests (SARs)

Under DPA1998, an individual may request a copy of any data held about them. **GDPR removes the £10 nominal fee** for making this request, which may increase the number of requests made.

### 2 Right to erasure

GDPR allows an individual to **request erasure** of their personal data, also known as right to be forgotten (RTBF). This is not absolute – an organisation may keep information if there is a business requirement to do so (e.g. statutory record keeping).

### 3 Consent

Consent to hold data must be by some affirmative action. Pre-ticked boxes, silence or inactivity are not sufficient (e.g. "Tick if you don't want to receive…" is no longer sufficient). Consent must also be verifiable and individuals have the option to withdrawn consent at any time. Existing data must have been acquired by a process which also meets the required standard of consent – or the organisation must stop processing it.

**More info: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/**

# GDPR COMPLIANCE ISSUES

The following is opinion based on Arena's understanding of GDPR requirements and compliance. It does not constitute legal advice and organisations are encouraged to seek further advice according to individual circumstances.

> Every organisation is responsible for ensuring both appropriate security of personal information and that only lawful processing takes place.

## Organisations will split into two broad groups:

**1. Business-to-business (B2B) organisations will hold personally identifiable data for those individuals involved in carrying on business. This will be largely employee/HR records and contact details of individuals with which the organisation trades.**

**a.** Employees will have all the rights of any person under GDPR – including rights of access and erasure, during and post-employment.

**b.** Named individuals at other organisations with which the organisation trades (e.g. customers, suppliers) will have personally identifiable data held – e.g. payment or delivery information – and consent will have been explicitly given by contracting with the organisation. The information will therefore be necessary for contract (hence unlikely to be subject to a right of erasure), but should be kept for no longer than is necessary.

**c.** Named individuals at organisations with which the organisation does not have a business relationship (e.g. prospecting/marketing databases) will have personally identifiable data held and this will be subject to the requirement for consent. Those individuals will have right of access and erasure and the organisation will not be able to claim a necessary business reason for retaining the data (unless the prospect has become a customer or was a customer, therefore the data is necessary for contract).

**2. Business-to-consumer (B2C) organisations will likely hold far more information.**

**a.** End-customers will be individuals and this increases the scale of the issues.

**b.** Particular care will be required when retaining customer information for marketing/repeat business purposes and whether customers are giving explicit consent for this (which must also be freely given and can't be assumed as part of the initial sale).

**c.** The points above for B2B organisations will also hold, for employees and trading with other organisations.

In both cases, every organisation is responsible for ensuring both appropriate security of personal information and that only lawful processing takes place.

## Definition of an individual

For the purposes of data protection legislation, an "individual" is a **living person.** The provisions are around data pertaining to living individuals, not companies, and this defines much of the scope of the legislation.

### Some potential pitfalls:

**a.** A complaint with respect to unsolicited marketing – can the organisation provide evidence that consent was given (freely, explicit)?

**b.** An ex-employee makes a right to be forgotten application – can the organisation easily locate all information relates to that individual, then efficiently determine which should be retained (e.g. statutory records) and which should be deleted?

**c.** A customer or ex-employee makes a Subject Access Request – again, can the organisation easily locate all relevant information and efficiently determine which must be provided to the individual and which should not (including redaction of confidential information which may be on the same documents). Note that at present SARs cost the individual £10, but under GDPR there is no cost.

# HOW ARENA CAN AID COMPLIANCE

It should be stressed that compliance with GDPR cannot be "bought" as a product-based solution and will only be achieved with a combination of awareness and appropriate processes. Technical solutions, such as the implementation of specially configured **m**store software, will simply make those processes practical and efficient.

## Consent Gathering

Arena has designed a consent gathering solution which can be delivered as a hosted/software-as-a-service solution. Briefly stated, this solution allows an organisation to confirm – using appropriate language – that an individual has provided consent for their data to be held and retains a record of that consent provision.

## Secure Copy and Print

Arena can help ensure that your copy, print and scan environment is robustly configured to minimise areas of risk. Also avoid data loss through unencrypted hard disk drives, USB ports and scan locations, all of which should be considered when creating a robust, compliant IT infrastructure.

Print management software allows documents to be securely released on demand to avoid sensitive documents being left on printers, and can provide insights into what information is disseminated in print format.

Data breaches often come from internal sources. Arena can help you put measures in place to help identify the source of a data breach should it originate from a printed document. Tools such as digital signatures on printed output enable you to identify who printed a leaked document and what else that user was printing leading up to the data breach thereby mitigating further risk of data loss. A print audit can also form part of the organisation's wider information audits to ensure you're on track for compliance.

> Arena provides a robust mechanism for consent gathering, which meets the standards set out in GDPR, without causing large amounts of work on the part of the processing organisation

# GDPR CONSENT GATHERING WITH MSTORE

1

The individual provides data – this will include a means of contact, either e-mail or mobile number (for SMS contact).

2


This data is entered to the consent-checking system – either manually or with a direct link. At this point the personal data is held in a waiting state.

3


The consent-checking system contacts the individual (via e-mail or SMS) with a link to a unique web page, where that individual confirms their granting of consent. This page will use specific text which explains what their information will be used for.

4


The individual confirms their consent and their information is released for processing.

5

The individual may return to the consent-checking system at a later date to retract their consent.

**This solution will provide a robust mechanism for consent gathering, which meets the standards set out in GDPR, without causing large amounts of work on the part of the processing organisation.**

mstore

# DATA MANAGEMENT

The **m**store EDRMS can be used to locate information related to individuals, then create workflows to manage processing of that information, assisting with SAR and right to be forgotten processing.

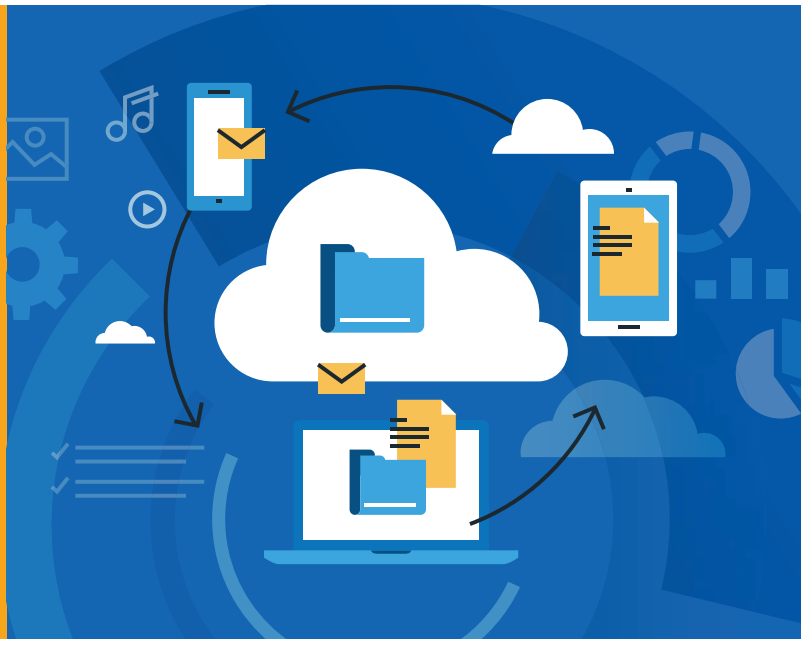
First, large amounts of information can be imported into **m**store and indexed for easy searching. Information can be classified into types (e.g. invoices, correspondence) and in some cases this classification can be used to quickly determine whether a document can be retained for genuine business reasons (e.g. an invoice for 6 tax years plus current) and therefore need not be considered in right to be forgotten processing. Further, a full-text index can be used to locate information related to an individual, even if the filing method (folder tags etc) does not include names. e.g. consider a legal case in the name of a company (hence filed by company) which makes reference to individuals (such as witnesses) and one of those individuals then requests to be forgotten. The full text index would quickly find all occurrences of that individual.

Once found, relevant documents can be placed into a workflow process which will manage the processing of that document. This will both aid in efficiency and serve as evidence of a formal process for handing SARs/RTBF requests.

Finally, **m**store provides tools for redaction of documents, to obscure data which cannot be shared (such as other names in the legal case/witness example above).

## Summary

GDPR is happening and will significantly impact on all organisations. Now is the time to act. As a minimum, every organisation should understand the changes to regulations around personal data and develop a clear in response to the changing legal requirements to protect them from risk. As a first step, getting your documentation in good order through effective implementation of an EDM solution whilst reviewing essential workflows is a step on the right direction which can stand up to scrutiny, protect your business, and enable a robust and timely response.



Speak to our experts to find out more: **0344 863 8000**
info@arenagroup.net | www.arenagroup.net