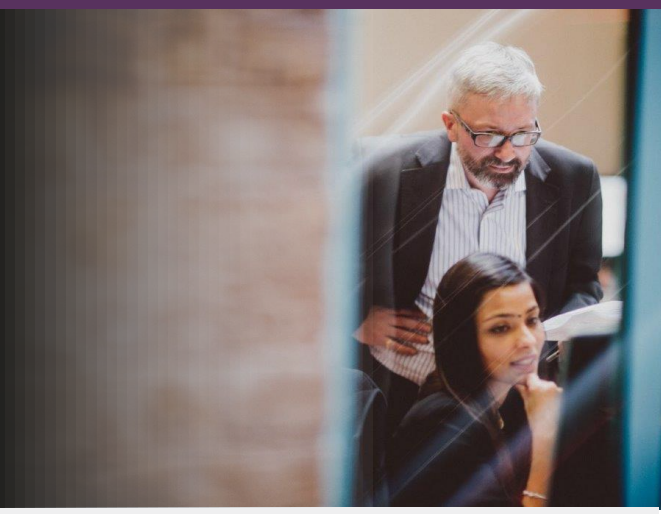
RIAA Barker Gillette

*Always Available*

# EU General Data Protection Regulation: What Do I Need to Know?



January 2017

## What Is EU General Data Protection Regulation (the GDPR)?

The aim of the GDPR is to harmonise the current data protection laws across the EU member states.

## When does the GDPR come into force?

The GDPR will apply in the UK from 25 May 2018. This is a significant change in data protection law and businesses will need to invest time preparing for the changes.

## Given Brexit, do you still need to prepare for compliance with the GDPR?

**YES**. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

To avoid being classified as inadequate, in terms of the level of protection given to personal data, the UK must offer data protection standards that comply with EU requirements. A company outside the EU with operations in the EU must also comply.

## Will consent given under an employment contract, by an employee to the processing of personal data, be sufficient?

The short answer is **NO**.

Under the GDPR, consent must be given:

- freely i.e. not as part of the employment contract;
- actively i.e. not simply 'by default'; and
- it must be as easy to withdraw as to give.

As an employee cannot usually reject a clause in their employment contract it is not (for GDPR purposes) considered to be 'freely given'. Therefore, silence, pre-ticked boxes or inactivity cannot constitute consent as these do not allow the employee to say no to an aspect of the proposed processing.

However, the GDPR does allow employers to rely on alternative valid bases for processing personal data (other than just employee consent). For example, where an employer need to process personal data to operate the payroll or the sick pay system. Employers can rely on the justification that such processing must happen for the employer to perform the employment contract.

## How will the GDPR change the rules regarding subject access requests?

A subject access request is a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under section 7 of the Data Protection Act 1998.

In standard cases, the current 40-day time limit for responding to subject access requests will be reduced to one month and the £10 fee will be revoked.

In complex cases, the one-month timeframe can be extended by a further two months and provision will be made for a fee to be charged if the request is clearly unfounded or excessive.

The GDPR will extend the right of access to personal data. Employees will be entitled to more information about how their data is handled, who has access to it, how long it is held for etc. Therefore, employers should ensure that anyone appointed to handle subject access requests has received up to date training.

## What steps should employers take to prepare for the GDPR coming into force?

The GDPR affects the whole of the business, but from an HR angle, we would suggest the following steps are taken as part of the overall business preparations:

1. **Audit HR data and data processes**

   Now is the time to assess what data is held by HR and how it is processed (who it is shared with and why?).

   What data protection policies and procedures do you currently have and are these working?

   Are there any risk areas that need attention before the GDPR comes into force?

2. **Audit your third-party processors**

   The GDPR contains increased obligations on employers to ensure that their third-party data processors comply with data protection laws. The obvious ones here include external payroll providers and occupational health assessors.

   You need to make sure that your contractual terms require third parties to comply with data protection law in processing personal data about your workforce.

   You should consider what steps you take to vet and check external service providers for compliance both prior to and during their appointment.

3. **Ensure staff are trained appropriately**

   General data protection training is as important as ever. Those with specific data processing responsibilities should be given additional tailored training.

4. **Move away from relying solely on employee consent to justify business critical data processing**

## Do you need to appoint a data protection officer?

The GDPR requires companies whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale to appoint a data protection officer. This person must have expert knowledge of data protection law and practices and their job will be to monitor internal compliance with the GDPR. Business who do not fall into this category may still wish to appoint someone to monitor data processing and keep a check on compliance.

For specific advice on your business needs in light of the GDPR please contact our employment team.

Note: This is not legal advice; it is intended to provide information of general interest about current legal issues.

**Karen Cole**
**020 7299 6909**
**karen.cole@riaabg.com**