Croner
HR • Tax • H&S • Reward

General Data Protection Regulation. It's almost here…

What is it?

The General Data Protection Regulation (GDPR) sets out the new rules for the lawful handling of data. You might already recognise this area of law as "data protection"; the GDPR will replace the current rules on data protection. This means you will need to change the way you currently deal with details you keep about your employees and report any significant data protection breaches. Certain businesses will need to appoint a Data Protection Officer to ensure compliance.

What is "data"?

An employee's name, address, photo etc. In fact, it is "any information relating to an identified, or identifiable natural person (data subject)".

Why is it happening?

It has become increasingly clear that the current statutory framework was not "fit for purpose". Personal data is now being used in ways that were not envisaged when the first Data Protection Act was introduced, mainly down to the growth of the internet and the changes in online activities.

When is it happening?

The new law will be introduced on 25th May 2018.

Do I have to do anything?

Yes, regardless of how small your business. GDPR will set legal requirements on employers because they fall into the group called "data controllers". There are huge penalties for non-compliance, including fines of up to €20 million or 4% of a company's global annual turnover. There is also a large focus on accountability.

Employee rights under GDPR

The right to be informed

Employees should be told the identity of the data controller and what their data is processed for. Employees must give free and specific consent for data to be processed

The right of access

Employees already have a right to see the data you hold on them but you will have to supply it sooner and won't normally be able to charge a fee anymore

The right to rectification

The right to object

The right to restrict processing

The right to data portability

The right to erasure

Individuals can request removal or deletion of data

Rights in relation to automated decision making and profiling

Preparing for GDPR implementation

The Information Commissioner's Office – the authority which governs data protection in Great Britain – sets out the following 12 steps that employers should take now to review their data protection practices in readiness for GDPR.

1. **Awareness** – let the relevant people in your organisation know that the law is changing

2. **Information audit** – check what data you hold and who you share it with

3. **Privacy information** – check your current privacy notices and make a plan for change

4. **Individuals' rights** – check how you currently comply with individuals' rights e.g. complying with a subject access request or deleting personal data

5. **Subject access requests** – plan how you will make changes to the process when the new law is here. Amend any standard documentation you have to comply with changes in current practice

6. **Lawful basis** – check you have a lawful basis for processing data. Employers who process data for employment purposes are likely to be able to rely on the lawful basis of "performance of a contract" for most data processing, but potentially not all processing

7. **Consent** – review how you obtain consent for processing data. This will include a review of employee handbooks, data protection policies and accompanying documentation

8. **Children** – reviewing procedures for verifying ages and obtaining parental/guardian consent (not likely to have a great impact on the area of employment)

9. **Data breaches** – review how you would notify a breach

10. **Impact assessments** – consider how to implement data protection impact assessments

11. **Data Protection Officer** – do you need a DPO? Who will ensure your compliance with GDPR?

12. **International** – If you operate in more than one member state, determine a lead data protection supervisory authority.

To speak to an expert call Croner on 0808 145 3490