General Data Protection Regulations – Employment

New data protection regulations are coming into force on 25th May 2018. Whilst that seems a long way off, businesses need to start taking action now to move towards compliance next year.

It applies to employers as they process personal data about their workers – personal data is general data about the individual and a special category of data which relates to particular characteristics (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation or sexual life and genetic and biometric data) - extra steps must be taken with regard to special category data.

The NTF will be issuing guidance over the coming months working through the different stages of what you need to do.

The new legislation will require privacy notices to be given to employees about how their personal data is used, the lawful basis for the business processing the information and the amount of time it will be retained, as opposed to the employee just giving blanket consent to it being used as at present.

Other key issues are that you have to be able to demonstrate compliance and if there is a data breach notify those affected by it. It will require you to have systems in place which are designed with privacy and data protection in mind.

As an initial step, we would advise that you decide who in the business will take responsibility for overseeing compliance with the new data protection regulations.

Once you have done that, the next step will be to audit what information your business currently holds. You can then consider what needs to be kept, why you need it and then move towards notifying employees about it.

Step 1 Appoint the person or persons responsible for data protection with your organisation

It is advised that someone is given overall responsibility to ensure that the data protection work is undertaken – however we recommend that you do not call them a data controller since this is a title that brings various obligations with it. We suggest just calling them the data protection manager or data protection leader.

<cont….>

Step 2 Arrange an audit of personal data your company holds

There is no set way of carrying out the audit but questions to be considered about the information held include:

- What kind of data is being collected, where and why?
- How is the data used (i.e. processed) both internally and externally?
- How long is the data retained?
- Who has access to the data both inside and outside of the business?
- What procedures and controls are in place to keep data safe?

The amount of time this may take should not be underestimated so that is why it is good to start now. Such data will include use of CCTV, sending payroll out to a third party provider and customer data bases – it is not just about employees.

Further information – which will be developed over the next few months as more guidance is issued by the Information Commissioners Office – is available on the NTF website in the employment area under General Data Protection Regulations. Members can find a suggested audit template and a link to the ICO website.