General Data Protection Regulations – Steps towards compliance

As members will know from previous newsletter articles, new data protection regulations - the General Data Protection Regulations - are coming into force on 25th May 2018. The organisation responsible for this is the Information Commissioner's Office (www.ico.org.uk).

Our advice on the GDPR is still being developed by way of template notices and policies but to ensure members can take steps towards compliance, we have set out below a timeline of steps to take.

The key concept of the new Regulations is that personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

Your business is accountable for these principles and you must be able to show that your business is compliant.

There is further information on the NTF website including a link to the Information Commission website and its advice on steps to take now.

Steps towards compliance

Before the end of March

- If you have not already done so, decide who is in charge of data protection in your company and ensure they are aware of GDPR and have started steps towards compliance.

- Review the personal data you currently hold within the business. This could relate to employees, customers, suppliers or people on your contact database. Note it only relates to living people, not companies. See "audit" advice on NTF website.

- As part of that exercise consider what you do with that data – what is your lawful reason for processing it? See "retention" advice on the NTF website.

- Ongoing – if you are installing new systems or setting up arrangements with third party providers such as payroll, benefit providers, occupational health, ensure they have adequate measures in place to protect employees' personal data and ensure that there are provisions in the contracts with those providers ensuring the safeguards are in place.

During April

- Establish your basis for processing data – see guidance on the NTF website. The existing consent you have from your employees in their employment contracts will not be sufficient valid consent after 25th May 2018.

- Look at what data do you give to third parties/share with others i.e. do you send your staff pay roll to an external company? If so, ensure they have adequate measures in place to protect employees' personal data and that there are provisions in the contracts with those providers ensuring the safeguards are in place. Check those provisions include how long they will keep any data after they have processed it.

- Look at what security arrangements you have in place around data – the NTF will be issuing advice upon this.

- What arrangements do you have to keep that data up to date? Consider having a diary system for checking with your employees that data is up to date – for example addresses, next of kin, driving licences for drivers etc.

- Review how you obtain, record and manage consent outside of the employment relationship. Where necessary refresh existing consents if they don't meet GDPR standards although in general, it is likely that you will rely upon the lawful basis for processing and documenting data through a privacy notice rather than using consent. Further guidance and templates will be issued by the NTF during April.

May

- Issue letter or other communication to existing employees enclosing Data Protection Privacy Notice – a template will be available on the NTF website during late April

- Ensure you have in place procedures to work out how you would handle a Subject Access Request – a template will be available on the NTF website during April

- Ensure that, if you have not already done so, your customers are aware of your data protection privacy notice – again a template will be available on the NTF website during April.

- Put in place procedures to detect, report and investigate personal data breaches – more information will be available on the NTF website.

- Create procedures to detect, report and investigate personal data breaches – more information to follow.

25th May 2018

GDPR regulations takes effect.

- Start using the new employment contracts available on the NTF website from that date.

- Check that employees, contractors and customers have all received their data privacy notices and/or your data protection policy.

- Remember that there may still be occasions where consent is needed – for example, if you wish to approach an employee's doctor for a medical report then you would need specific consent from the employee under the Access to Medical Records provisions (chapter 10 of the NTF employment guide).

Going forward

- Ensure that your policies are followed.

- Remember to delete data no longer needed from all places.

- Remember to keep records so that you can show that you are compliant with the data protection principles.

- Ensure that any breaches are dealt with and notified to the data subject.

- Respond promptly to any Subject Access Requests.

NTF

March 2018