GDPR PLANNING CHECKLIST

The GDPR takes force from 25 May 2018. You should start planning so that on that date you can demonstrate compliance with the GDPR. Businesses are expected to put into place comprehensive but proportionate governance measures.

The following checklist will allow you to prepare for the GDPR by documenting existing procedures, looking for areas to strengthen. You will need to use your judgement to confirm you have proportionate governance measures if you complete the planning yourself or you may choose to use an external consultant. Document the actions you are planning to take and note the changes.

1. Review all data held and ask "why is it held?" and "do you still need it?" and "is it safe?" Make sure you note the different sorts of data you hold e.g. employees, customers, suppliers, third parties;

2. Look at your consent procedures as well as privacy notices on your web site and terms of business. Do you get customers to positively agree to you holding their data;

3. Document the reasons you hold data e.g. consent, legitimate interests or a legal obligations to collect and process data;

4. Plan how you will handle data requests and the right to be forgotten from individuals within the new timescales;

5. Look at your processes to keep data safe, identify any problem areas (e.g. data held on mobile devices) and decide how you can reduce the risk of data breaches (e.g. encryption). This will mean looking also at your back-up security of data, computer and passwords and identifying new technology to help you comply with the GDPR;

6. Document the procedures you have in place to detect, report and investigate data breaches and let everyone in your business know about your new data protection policy;

7. Consider who in your business will be the person responsible for the GDPR and making sure all employees are aware of the new regulations and ensuring compliance.