General Data Protection Regulations

What is GDPR?

- A regulation responding to the change in how individuals and organisations now interact
- One of Data Protection Acts '8 principles of data protection', which explains all personal data must be processed lawfully, fairly and for the purpose for which it was given.
- It will be introduced from 25 May 2018, and will continue to stay in place in the UK post-Brexit as the UK government will introduce a new Data Protection Bill.
- There will be no exceptions for any industry.

What is Personal Data?

- Any data which relates to or identifies a living person.
- The GDPR will expand the definition of personal data to include location data and biometric data.
- Sensitive data relates to an individual's race, health, sexual orientation, religion and political views, trade union membership and criminal records – this must be given at a higher level of protection.
- A data subject is the person whom the personal data relates.

New Rights for Individuals

- Express Consent: This is information which is actively and freely given, however legitimate interest is an alternative to consent though it can only be used where appropriate. Legitimate interest could be used to provide work-finding services generally, but express consent would be required to transfer personal data from another party such as an umbrella company.
- Withdraw Consent: Individuals will have the right to withdraw consent, which should be as easy as giving consent. You must tell individuals that they have this right.
- Rectification: Requesting incorrect data to be corrected by the organisation holding it. Then notifying any parties this data was transferred to and checking the data has been rectified.
- Erasure: Requesting that their data is removed along with any transferred data. However, this is not an absolute right and so must be balanced against other records such as payroll, working time records or safeguarding records.
- Data Portability: Allows an individual to bring their personal data from one data controller to another. This must be given in a 'structured', commonly used and machine-readable format.

New Obligations on Organisations

- Consent: Need to be express consent in order to process data.
- No longer able to rely on pre-ticked or opt-out boxes, however you may be able to rely on legitimate interest to process data.
- Appointing a company data protection officer: Due to the nature and volume of personal data, a DPO must have sufficient authority and resources to be able to do their job properly. The DPO will not be liable if the company breaches the GDPR, as liability is with the organisation.
- If you decide not to appoint a DPO, somebody must be responsible for managing data protection within the organisation.
- Subject access requests: The right to request to find out what data an organisation holds on an individual. Organisations will no longer be able to charge for S.A.R, except where the individual makes repeated or unfounded S.A.R's. They must respond within 1 month, however this can be extended to 2 months where the request is particularly complex.
- Automated Decision Making: Individuals should not be subjected to automated decision making.
- Liability for Data Breaches: Ensuring any party's personal data is transferred to be also following the GDPR. If an individual suffers damage as a result of a transfer of their data, any

organisation involved in the transfer may be liable for the breach. E.g. Using payroll intermediaries such as umbrella companies will have to be express consent in order to transfer data. Consent hidden in Terms and Conditions are not express nor freely given.

- Accountability Principle: Organisations must show that they comply with the GDPR. They must have a process in place to inform individuals of their rights, manage requests to withdraw consent, or rectify or delete data when requested. They must also report data breaches within 72 hours of becoming aware of the breach.
- Sanctions for non-compliance: The GDPR allows members states to apply appropriate administrative fines for lesser breaches. They can be fined up to 20 million Euros or 4% of annual worldwide turnover (whichever is highest) – this will apply to the most serious breaches.