GDPR CHECKLIST

Have you

- Documented your decision on whether or not to appoint a DPO or other responsible person for managing data protection? **YES/NO**
- Conducted a data audit of existing employee / customer / supplier data? **YES/NO**
- Documented your handling of personal data? **YES/NO**
- Identified your lawful bases for processing, storing, and documenting personal data? YES/NO
- Documented how you request and record consent? **YES/NO**
- Written your data protection policy and communicated it to all members of the business in a variety of formats (booklet, wall poster, website, etc.)? **YES/NO**
- Communicated protocols for handling sensitive personal data where relevant? **YES/NO**
- Implemented and documented personal data and IT security measures (restricted access, passwords, data encryption, antivirus and firewall software,etc.)? **YES/NO**
- Developed a procedure for identifying, communicating, containing, resolving, and reporting any data breaches? **YES/NO**
- Provided data handling, data protection, and breach management training for current and new staff? **YES/NO**
- Communicated privacy notices that clearly explain *how* and *why* the personal data of employees, customers, suppliers, job applicants, et al, is collected, used, and stored? **YES/NO**
- Communicated protocols for data rectification, personal access, data quality, and erasure where it's allowable? **YES/NO**

- Provided clear consent requests on all communications including your website and offline marketing? **YES/NO**

SOME DATA PROTECTION TIPS

EMAILS. Before opening any email make sure you know who sent it. If you don't know the source, delete it without opening it. Avoid opening and sending emails by phone as it can be more difficult to check that email addresses and attachments are correct. At work use only your company's official email system and observe any protocols that are in place.

DOWNLOADS. Have robust antivirus software in place and be sure to update it before you sign up for and download any third party app or file. If you're using a computer at work you should check that you're not about to violate your company's data security protocols.

SENSITIVE DATA. If you have received sensitive data legitimately you should ensure that it's secure and avoid sharing it without the owner's permission. If you received the data by accident you should inform the sender and delete it securely.

TRANSFERING PERSONAL DATA TO A THIRD PARTY. Before going ahead make sure you have the data owner's written consent. Don't breach your company's data protection policy - make sure you're sending the data to an approved third party and you're using an approved secure transfer solution.

CARRYING PERSONAL DATA. When out and about you must exercise due care attention to avoid loss or theft of any personal data you may be carrying. Don't be careless with data - remain alert and avoid distractions when you're in a public space. Don't leave personal data visible on screen or paper unnecessarily. Lock your mobile or laptop and put your papers in your briefcase when you're done with them. Avoid any temptation to walk away and leave them unattended "just for a minute or two".

TALKING. Avoid 'sensitive' talk where others may hear. If you must discuss personal data in a public space, watch what you're saying and how loudly you say it.

PUBLIC WIFI. If you need to go online to access personal data, use a VPN (Virtual Private Network) that encrypts data even when connected to a password-protected network. Don't connect to an unsecured WiFi network.

DATA DISPOSAL. Don't keep personal data longer than is necessary. If you don't need confidential papers, shred them before bagging and binning them. Use a reputable virtual shredder to securely delete confidential emails and electronic documents.

THINK DATA PROTECTION. Read and re-read your employer's data protection policies and procedures (or write and re-write your own if self employed) to keep data protection always in mind.